An Economic Study of the Effect of Android Platform Fragmentation on Security Updates

Sadegh Farhang[1], Aron Laszka[2], and Jens Grossklags[3]

[1] Pennsylvania State University
[2] University of Houston
[3] Technical University of Munich
farhang@ist.psu.edu, alaszka@uh.edu, jens.grossklags@in.tum.de

Abstract. Vendors in the Android ecosystem typically customize their devices by modifying Android Open Source Project (AOSP) code, adding in-house developed proprietary software, and pre-installing third-party applications. However, research has documented how various security problems are associated with this customization process.

We develop a model of the Android ecosystem utilizing the concepts of game theory and product differentiation to capture the competition involving two vendors customizing the AOSP platform. We show how the vendors are incentivized to differentiate their products from AOSP and from each other, and how prices are shaped through this differentiation process. We also consider two types of consumers: security-conscious consumers who understand and care about security, and naïve consumers who lack the ability to correctly evaluate security properties of vendor-supplied Android products or simply ignore security. It is evident that vendors shirk on security investments in the latter case.

Regulators such as the U.S. Federal Trade Commission have sanctioned Android vendors for underinvestment in security, but the exact effects of these sanctions are difficult to disentangle with empirical data. Here, we model the impact of a regulator-imposed fine that incentivizes vendors to match a minimum security level. Interestingly, we show how product prices will decrease for the same cost of customization in the presence of a fine, or a higher level of regulator-imposed minimum security.

1 Introduction

Android, the mobile operating system released under open-source licenses as the Android Open Source Project (AOSP), has the largest market share among smartphone platforms worldwide with more than one billion active devices [2]. Due to the openness of the platform, vendors and carriers can freely customize features to differentiate their products from their competitors. This differentiation includes customizing the hardware, but there is also a substantial fragmentation in the software packages utilized in the Android ecosystem [15, 22].

The fragmentation of the software base available from various vendors is due to various customization steps, including the modification of the open source

Android codebase as well as the addition of proprietary software. Product differentiation may benefit consumers by providing Android devices for sale that better match consumer tastes, and may also benefit businesses by helping them to sidestep intense price competition of homogeneous product markets [24].

However, we also observe that Android platform fragmentation is associated with a number of security challenges [23, 25, 26]. For example, Wu et al. showed that a large proportion of security vulnerabilities in the Android ecosystem are due to vendor customization. They calculated that this proportion is between 64% to 85% for different vendors [25]. Similarly, Zhou et al. showed how customized drivers for security-sensitive operations on Android devices available by different vendors often compare unfavorably to their respective counterparts on the official Android platform [26]. Thomas et al. provided evidence for the substantial variability of security patch practices across different vendors and carriers [23]. Using a dataset about over 20,000 Android devices, they showed that on average over 87% of the devices are exposed to at least one of 11 known critical (and previously patched) vulnerabilities.[4]

The Android ecosystem fragmentation and the associated security problems have caused consumer protection agencies to intervene in the marketplace. In 2013, the Federal Trade Commission (FTC) charged a leading vendor because it "failed to employ reasonable and appropriate security practices in the design and customization of the software on its mobile devices" [9]. The case was settled and the vendor was required to "establish a comprehensive security program designed to address security risks during the development of new devices and to undergo independent security assessments every other year for the next 20 years" [9]. Not observing significant improvements in the Android ecosystem, the FTC recently solicited major vendors to provide detailed information about their security practices including what vulnerabilities have affected their devices as well as whether and when the company patched those vulnerabilities [8].

In this paper, we propose a product differentiation model that captures key facets of the Android ecosystem with a focus on the quality of security. We consider multiple competing vendors, who can customize Android for their products in order to differentiate themselves from their competitors. We consider both security-conscious consumers, who value security quality, and naïve consumers, who do not take security issues into consideration when they make adoption choices. When consumers are naïve, vendors do not have any incentives to address security issues arising from the customization. In order to incentivize investing in security, a regulator may impose a fine on vendors that do not uphold a desired level of security. We show that fines can achieve the desired effect, and we study how they impact the competitive landscape in the Android ecosystem.

Roadmap. In Section 2, we provide background on Android customization and the associated security challenges. Section 3 presents the economic model on Android customization. We analyze the model without a fine in Section 4 and

[4] Further compounding the problem scenario is how third-party apps targeting outdated Android versions and thereby disabling important security changes to the Android platform cause additional fragmentation [19].

consider how to calculate the parameters in our model in Section 5. We extend the model to the case with a regulator-imposed fine in Section 6. We support our analysis with numerical results in Section 7. We conclude in Section 8.

2 Background

Customization: One approach to measure the level of customization by vendors is *provenance* analysis [25], which studies the distribution and origin of apps on Android devices. There are mainly three sources of app origins on Android devices: (1) AOSP: apps available in the default AOSP that, however, can be customized by a vendor; (2) Vendor: apps that were developed by that vendor; and (3) Third-party: apps that are not in AOSP and were not developed by the vendor.

Table 1 summarizes the published findings of a provenance analysis of five popular vendors: Google, Samsung, HTC, Sony, and LG [25]. The authors found that on average 18.22%, 64.41%, and 17.38% of apps originate from AOSP, vendors, and third parties, respectively. Further, the number of apps and lines of code (LoC) associated with the devices are increasing with newly released versions. Likewise, the complexity of the baseline AOSP is increasing over time [25].

					AOSP		**vendor**		**3rd-party**	
Vendor	**Device**	**Version and Build#**	**#apps**	**#LOC**	**#apps**	**#LOC**	**#apps**	**#LOC**	**#apps**	**#LOC**
Samsung	Galaxy S2	2.3.4; 19100XWKI4	172	10M	26	2.4M	114	3.5M	32	4.1M
Samsung	Galaxy S3	4.0.4; 19300UBALF5	185	17M	30	6.3M	119	5.6M	36	5.3M
HTC	Wildfire S	2.3.5; CL362953	147	9.6M	24	2.7M	94	3.5M	29	3.3M
HTC	One X	4.0.4; CL100532	280	19M	29	4.7M	190	7.3M	61	7.5M
LG	Optimus P350	2.2; FRG83	100	6.1M	27	1.1M	40	0.6M	33	4.4M
LG	Optimus P880	4.0.3; IML74K	115	12M	28	3.1M	63	3.2M	24	5.6M
Sony	Xperia Arc S	2.3.4; 4.0.2.A.0.62	176	7.6M	28	1.1M	123	2.6M	25	3.8M
Sony	Xperia SL	4.0.4; 6.1.A.2.45	209	10M	28	1.8M	156	4.1M	25	4.7M
Google	Nexus S	2.3.6; GRK39F	73	5.2M	31	1M	41	2.8M	1	1.3M
Google	Nexus 4	4.2; JOP40C	91	15M	31	2.5M	57	12M	3	1.1M

Table 1. Provenance analysis [25].

One of the challenges in this fragmented ecosystem is the security risk that arises from the vendors' and carriers' customization to enrich their systems' functionality without fully understanding the security implications of their customizations. In this paper, our focus is on security issues resulting from such customization. We provide an overview of relevant work in this area in the following subsection.

Security Impact of Customization: The problems related to security aspects of Android customization are mainly due to vendors' change of critical configurations. These changes include altering security configurations of Linux device drivers and system apps, etc. One approach for better understanding the effect of customization is to compare security features of different Android devices with each other, which is called differential analysis. Aafer et al. proposed a number of security features to take into account [1]. First, *permissions* which protect data, functionalities, and inner components can be analyzed. In Android, we have four level of permissions: *Normal*, *Dangerous*, *Signature*, *SystemOrSignature*. The goal of differential analysis is to find a permission with a different (and typically lower) level of protection on some devices. Second, group IDs (*GIDs*) are another feature to take into account. Some lower-level

GIDs are given Android permissions, which could potentially be mapped into a privileged permission due to customization. Protected broadcasts sent by system level processes are a third important security feature. Due to customization, some protected broadcasts could be removed and, as a result, apps can be triggered by not only system-level processes but also by untrusted third-party apps.

By comparing these security features, Aafer et al. found that the smaller the vendor is, the more significant inconsistencies are observable for the different security features. One interpretation is that the cost of investment in security is too high for those vendors (e.g., hiring of security experts). The results also imply that different vendors invest in security to different degrees.

Research aiming to understand Android customization is clearly demonstrating that customization is a pervasive feature in Android, and this is associated with a wide variety of security challenges and vulnerabilities. Further, we are unaware of any research that provides evidence for security improvements resulting from customization, which outweighs the aforementioned risks. At the same time, research is missing that aims to understand the economic forces associated with the customization process, which is the objective of our work.

Product Differentiation: Hotelling proposed a widely cited model for product differentiation in which a linear city of fixed length lies in the horizontal axis, and consumers are distributed uniformly in this interval [16]. Firms strategically chose a location in this space, since consumers appreciate firms who are closer to their location. We draw from this basic setup, and a more tractable extension using a quadratic function for consumer preferences for distance [5, 24]. An alternative product differentiation model was proposed by Salop with consumers located uniformly on a circular city [21]. These two models are typically referred to as spatial competition or horizontal differentiation. In contrast, vertical (quality) differentiation has been used to formalize quality competition [11]. Our model also draws on quality differentiation by considering different levels of security investments by Android vendors.

Another type of (*perceived*) product differentiation is related to the lack of complete information about the characteristics of different products by consumers, which is called *information differentiation*. Advertising is a key factor affecting the perceived product differentiation and resulting consumer demand [24]. Kaldor [17] proposed that advertising yields information benefits to consumers, while other researchers suggest that advertisement misleads consumers [12, 24]. In our model, we take the view that consumers are largely uninformed about the security quality of Android devices by different vendors when they make adoption decisions. We are unaware of any research studying explicitly users' awareness of Android OS security, however the recent FTC request for information from Android vendors provides indirect evidence of the opaqueness of Android security practices [8]. In addition, a multitude of papers have addressed lack of awareness about third-party app security (e.g., [20]). While we believe that at least a small segment of consumers is concerned about Android security, and takes proactive steps to inform themselves (see, for example, the following paper on Android permissions [10]), we defer research on populations with mixed levels of security-awareness to future work.

3 Model Definition

In this section, we propose our baseline model in the tradition of *game theory* and the *theory of product differentiation* [16, 24]. Our model considers three types of entities: (1) AOSP, (2) vendors, such as Samsung or LG, and (3) consumers.

AOSP: Google, the developer of Android, provides monthly security updates for its devices and for base Android. However, other vendors have to adjust AOSP security updates for their Android devices because of their customization. Further, customization may also introduce new security vulnerabilities.

To incorporate these effects into our model, we assume that a customized version of Android can be represented by a point on the segment $[0, 1]$. Our analysis could be extended to multidimensional customizations in a straightforward way, but we assume one dimension for ease of presentation, since our focus is on the relative level of customization rather than its direction. Moreover, the location of each Android customization is independent of objective measures of product quality. In other words, we map the features of a mobile device to a point on the segment $[0, 1]$ to quantify its difference (e.g., percentage of customized code) from the base version of Android provided by AOSP. In our model, Z_A denotes the point corresponding to the base version of AOSP. Since AOSP aims to provide a base version that maximizes the market share of Android, it provides a version that can attract the widest range of consumers. Hence, in the numerical analysis, we assume that AOSP is in the middle, i.e., $Z_A = 0.5$.

Vendor: There are multiple vendors selling Android devices. Likewise, carriers can also sell the vendors' Android devices with their own prices and customizations. Here, we will use the term "vendor" to refer to both vendors and carriers. The price and the market share of the device sold by vendor i are denoted by p_i and D_i, respectively. Further, q_i denotes the security quality of patches delivered by vendor i. We assume that $p_i \geq 0$ (product prices are non-negative) and $q_i \geq 0$ (security quality is represented by a non-negative number) for every vendor i. Similar to the AOSP base version, a point $z_i \in [0, 1]$ represents the customization of the Android version of vendor i.

We consider two types of costs for customization. First, through customization, the vendor makes its product different from what Google has developed in AOSP. Hence, the vendor incurs development cost, which is related to the degree of customization. Here, we model this cost as a convex quadratic function of the difference between the vendor's position and the positions of the AOSP base version. Second, the security related cost of a vendor depends not only on the quality and frequency of security updates provided by the vendor, but also on the difference due to customization. Vendors receive security patch updates from AOSP, but due to customizations, vendors need to adapt these security patches before distribution. Often, vendors degrade the quality or frequency of security patches in order to save development and distribution costs [23]. Hence, the security-related cost is affected by both the customization level and the security quality. In our model, we employ a convex quadratic function to capture how the security cost of vendor i depends on q_i. The utility of vendor i is equal to:

$$\pi_i = p_i D_i - C_i \left(z_i - Z_A\right)^2 - S_i q_i^2 \left(z_i - Z_A\right)^2 , \tag{1}$$

where C_i and S_i are constants representing cost per unit of customization and security quality, respectively. Note that we focus on security issues resulting from Android customization rather than security-related cost of AOSP.

We have considered quadratic functions for the cost terms, which is a common assumption for modeling customization costs, e.g., see [4] and [6]. The quadratic cost function captures the fact that the cost of customization increases as the customization increases. In a similar way, with an increase in the cost of customization or the quality of security, the security cost resulting from customization increases. It would be possible to use any functional form with increasing marginal cost, such as an exponential cost function, which would lead to the same qualitative results as the ones presented here.

We also consider the quality of security patch updates provided by AOSP, denoted by Q, to be an exogenous parameter in our model, which applies to all vendors in the same way. Note that we observe that in practice, vendors virtually never provide better security quality. Further, we are primarily interested in studying the effect of customization on security; hence, we will not consider vendors implementing additional security measures that are independent of customization. Hence, we assume that the value of q_i is upper bounded by Q.

Consumers: Consumers choose mobile devices primarily based on prices and how well the devices match their preferences, but they may also consider security quality. A consumer's preference, similar to a vendor's customization, can be represented by a point x in $[0, 1]$. Consumers' preferences for smartphone selection are heterogeneous and we assume that the consumers' preferences are distributed uniformly in $[0, 1]$. We consider security-conscious consumers who take security into account when choosing their product. The utility of consumer j for choosing Android type i given that consumer j is at x_j is:

$$u_j^i = \beta q_i - p_i - T \left(x_j - z_i\right)^2 , \tag{2}$$

where T represents the consumer's utility loss for one unit of difference between its preference and the location of the product, which we call *customization-importance*. Similarly, β represents the consumer's utility gain for one unit of security quality, which we call *security-importance*. Naïve consumers, who do not understand or care about security quality, can be modeled by letting $\beta = 0$.

Our utility for consumers is in agreement with literature in economics [5]. It is common to consider quadratic term in economics to model utility.

Game Formulation: For tractability, we consider a two-player game between vendor 1 and vendor 2 without any other vendors.[5] In our analysis, we

[5] While we restrict our model to two vendors, we are aware that in practice, there are more than two vendors competing with each other. However, we believe that

assume that vendors are on different sides of AOSP. Further, we let $a = z_1$ and $1-b = z_2$. Without loss of generality, we assume that $0 \leq a \leq 1-b \leq 1$. Figure 1 shows the location of vendor 1 and vendor 2.

The utilities of vendors 1 and 2 are then as follows:

$$\pi_1 = p_1 D_1 - C_1 \left(a - Z_A\right)^2 - S_1 q_1^2 \left(a - Z_A\right)^2, \tag{3}$$

$$\pi_2 = p_2 D_2 - C_2 \left(1 - b - Z_A\right)^2 - S_2 q_2^2 \left(1 - b - Z_A\right)^2. \tag{4}$$

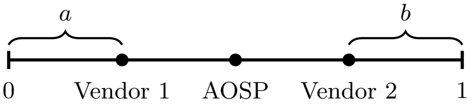


Fig. 1. Location of vendor 1 and vendor 2.

To calculate the Nash equilibrium, we need to define the stages of the game, i.e., the order in which the two players choose their prices, locations, and security levels. For our analysis, we consider the following stages:

- **Stage 1**: Both vendors simultaneously choose their location parameters a and b. They also choose their level of security quality, i.e., q_1 and q_2.
- **Stage 2**: Both vendors simultaneously choose their prices p_1 and p_2.

The reason is that a vendor freely modifies the AOSP code base, adds its developed proprietary software, and installs a diverse set of third-party apps to customize its device. These changes, however, result in the change of critical configurations leading to security issues [23, 25, 26]. Therefore, it is reasonable to consider that the customization and security quality effort happen at the same stage. Then, by taking into account its effort in customization and security quality, the vendor chooses its price. We use backward induction to solve our game. First, we consider stage 2 and calculate the price Nash equilibrium for given locations and quality. Then, we consider stage 1 and calculate the location and quality equilibrium assuming a price equilibrium in stage 2.

Table 2 shows a list of the symbols used in our model.

4 Analytical Results

In this section, we analyze our proposed model. Before considering the two stages, we first have to find the market shares of both vendors. To do so, we need to find the point in which a consumer j is indifferent between choosing vendor 1's product and vendor 2's product. This means that a user's preference at this point is identical for the two products. Hence, we have:

$$u_j^1 = u_j^2 \;\Rightarrow\; \beta q_1 - p_1 - T\left(x_j - a\right)^2 = \beta q_2 - p_2 - T\left(1 - b - x_j\right)^2. \tag{5}$$

similar to classic economic studies with two companies in the context of product differentiation, our model provides a meaningful understanding of the customization in the Android ecosystem and of security quality.

Table 2. List of Symbols

Symbol	Description
Z_A	Point corresponding to AOSP
D_i	Market share of vendor i
z_i	Customization of the Android version of vendor i
p_i	Price of vendor i
q_i	Security quality of patches delivered by vendor i
S_i	Cost per unit of security quality
C_i	Cost per unit of customization
π_i	Utility of vendor i
Q	Quality of security patch updates provided by AOSP
β	Consumer's security-importance
T	Consumer's customization-importance
x_j	Consumer's location
u_j^i	Utility of consumer j for choosing Android type i
q^{min}	Minimum level of security from the regulator's point of view
f_i	Fine function for vendor i
F	Monetary value of fine for each unit of violation from q^{min}

Solving the above equation yields:

$$D_1 = x_j = a + \frac{1-a-b}{2} + \frac{\beta\left(q_1 - q_2\right)}{2T\left(1-a-b\right)} + \frac{p_2 - p_1}{2T\left(1-a-b\right)}. \tag{6}$$

All of the consumers that are on the left side of x_j choose the product of vendor 1. As a result, the market share of vendor 1 is $D_1 = x_j$. This means that for equal prices and security qualities, vendor 1 controls its own "turf" of size a and the consumers located between vendor 1 and vendor 2 that are closer to vendor 1 than vendor 2. The last two terms represent the effect of security quality and price differentiation on the demand, respectively.

We restrict the model to consumers who definitely choose between these two products, which is a reasonable assumption for a wide range of parameters given the "cannot-live-without-it" desirability of modern phones, which is a valid assumption in economics, see [24]. Hence, the remaining consumers choose vendor 2's product, and its demand is accordingly:

$$D_2 = 1 - D_1 = b + \frac{1-a-b}{2} + \frac{\beta\left(q_2 - q_1\right)}{2T\left(1-a-b\right)} + \frac{p_1 - p_2}{2T\left(1-a-b\right)}. \tag{7}$$

If two vendors are at the same location, they provide functionally identical products. For a consumer who takes into account customization, price, and security quality, the factors that matter in this case are security quality and price. To increase their market share, vendors have to decrease their prices or increase their security quality. This will lead to lower product prices and higher costs due to higher security quality, and significantly lower – and eventually zero – utility for both vendors. Hence, vendors have no incentives for implementing customizations that result in identical product locations.

Price Competition: In the following, we state the price Nash equilibrium.

Theorem 1 *The unique price Nash equilibrium always exists, and it is*

$$p_1^* = \frac{\beta}{3}\left(q_1 - q_2\right) + T\left(1 - a - b\right)\left(1 + \frac{a - b}{3}\right), \tag{8}$$

$$p_2^* = \frac{\beta}{3}\left(q_2 - q_1\right) + T\left(1 - a - b\right)\left(1 + \frac{b - a}{3}\right). \tag{9}$$

The proof of Theorem 1 can be found in the extended version of the paper [7].

In Theorem 1, the price of a product depends on both the security quality and the customization level of both vendors. Further, the price depends on the customization importance T and security-importance β constants, which model the consumers in our model. A vendor can increase its price by improving its security quality or customizing its devices more.

Quality and Product Choice: To calculate the Nash equilibrium of both vendors in terms of location and security quality, we consider the following optimization problems.

Vendor 1 maximizes its utility in q_1 and a considering that p_1 is calculated according to Equation 8. For vendor 1, we have:

$$\begin{aligned} &\underset{a,\, q_1}{\text{maximize}} && p_1^* D_1 - C_1\left(a - Z_A\right)^2 - S_1 q_1^2\left(a - Z_A\right)^2 \\ &\text{subject to} && p_1^* \geq 0, \quad 0 \leq a \leq Z_A, \quad 0 \leq q_1 \leq Q. \end{aligned} \tag{10}$$

The constraints in the above optimization problem reflect our previous assumptions about the parameters in our model definition. For each value of b and q_2, the solution of the above optimization problem provides vendor 1's best response. In a similar way, for vendor 2, we have:

$$\begin{aligned} &\underset{b,\, q_2}{\text{maximize}} && p_2^* D_2 - C_2\left(1 - b - Z_A\right)^2 - S_2 q_2^2\left(1 - b - Z_A\right)^2 \\ &\text{subject to} && p_2^* \geq 0, \quad 0 \leq b \leq Z_A, \quad 0 \leq q_2 \leq Q. \end{aligned} \tag{11}$$

For given values of a and q_1, the above optimization problem provides vendor 2's best response. Based on the Nash equilibrium definition, the intersection of these two optimization problems gives the Nash equilibrium of our proposed game, i.e., a^*, b^*, q_1^*, and q_2^*. In the extended version of the paper [7], we provide our method for solving these two optimization problems and for finding the Nash equilibrium.

Lemma 1 *When consumers take into account security, zero investment in security for both vendors, i.e., $q_1 = q_2 = 0$, is not a Nash equilibrium.*

The proof of Lemma 1 is provided in the extended version of the paper [7].

The above lemma shows that when consumers take into account security, then vendors have to invest to improve their security quality. However, it is challenging for the majority of consumers to measure by themselves the security quality of a product, or in this case, to make a comparison between the security quality of many customized versions of Android provided by the vendors. Consumers mainly rely on information that is made available to them.[6] However, in the absence of any reliable market signal, any unsubstantiated communication/advertisements by vendors about security quality have to be considered with caution.[7]

Previous research has shown that businesses aim to exploit such information barriers. In particular, the theory of *informational market power* posits that when it is hard for consumers to understand and/or observe certain features of a product (e.g., security quality), then businesses are incentivized to underinvest in these product features and rather focus on easily observable aspects such as product design and price [3].[8] Any effect of informational market power is emphasized by well-known human biases such as *omission neglect* [18]. This describes the human lack of sensitivity about product features that are not the focus of advertisements or product communications; to paraphrase, consumers will often not consider in their *perceived utilities* product features which are not emphasized. Therefore, we consider an important baseline case of naïve consumers. In particular, we show that our model is in agreement with what we have seen in practice, i.e., vendors do not invest in security when consumers are naïve. Further, we determine under what conditions maximal differentiation, i.e., $a^* = b^* = 0$, is Nash equilibrium; see the extended version of the paper [7].

5 Parameter Selection

In the previous section, our analyses were focused on six variables: p_1, p_2, q_1, q_2, a, and b. In addition to these six variables, we have six parameters, which are β, T, C_1, C_2, S_1, and S_2. In this section, we discuss how we can quantify these six parameters in practice. In doing so, we use a reverse approach. First, we measure the values of p_1, p_2, q_1, q_2, a, and b. Then, based on our analyses in the previous section, we calculate the values of the constants in our model.

Location Quantification: In order to quantify customization and map it to a location, we need to quantify how different two Android versions are in terms of pre-loaded apps. To do so, we can access the image of an Android OS version, e.g., see [25] and [1], and investigate how many apps a vendor has developed for a specific version.

[6] While we have identified a small set of research projects which aim to understand the security impact of customization, e.g., [23, 25, 26], we are unaware of any well-known market signals regarding the security of different Android versions. The recent FTC initiative to solicit security-relevant data from vendors may contribute to such signals in the future [8].

[7] In fact, research by Wu et al. shows that vendors of different reputation (which may also influence perceptions regarding Android security) all suffer from similar challenges due to Android customization [25].

[8] Note that it is not required that businesses have an accurate assessment of the security quality of their own product (or competitors' products) for informational market power to be exploited.

					AOSP		vendor		3rd-party	
Vendor	**Device**	**Version and Build#**	**#apps**	**#LOC**	**#apps**	**#LOC**	**#apps**	**#LOC**	**#apps**	**#LOC**
HTC (vendor 1)	One X	4.0.4; CL100532	280	19M	29	4.7M	190	7.3M	61	7.5M
Samsung (vendor 2)	Galaxy S3	4.0.4; 19300UBALF5	185	17M	30	6.3M	119	5.6M	36	5.3M

Table 3. Origin of apps in two devices [25].

To quantify customization, we use the results of Table 3 and calculate the proportion of the code that was developed by a vendor. Note that in our model, we assume that the locations are in the interval $[0, 1]$. First, we need to specify the location of Z_A and then select the locations of the other vendors. Here, we assume that $Z_A = 0.5$. For the HTC One X (i.e., vendor 1), 7,354,468 LoC were developed by the vendor and 7,550,704 LoC stem from third-party apps. This means that about 75.95% LOC were added by that vendor to the baseline AOSP version. Here, we interpret this number as the level of difference between the device and AOSP. In order to keep the value of a in the interval $[0, 0.5]$, we let $a = Z_A - (percentage/2)$. Therefore, we have $a = Z_A - (0.7595/2) = 0.1203$. In a similar way, for the Samsung Galaxy 3 (i.e., vendor 2), 5,660,569 LOC were developed by the vendor in addition to 5,334,152 LoC coming from third-party apps, which is equal to 63.41% of the total number of LOC. In a similar way, we let $b = 1 - Z_A - (0.6341/2) = 0.1830$.

Quality: To quantify q_1 and q_2, we use the analysis reported in [25]. For a sample of 10 devices, they found that the maximum number of vulnerabilities for a device is 40. Some of these vulnerabilities are the result of vendor customization. For the HTC One X, 15 vulnerabilities were found, and 10 of these vulnerabilities are due to vendor customization. By dividing the number of vulnerabilities resulting from customization with the maximum number of vulnerabilities, we get 0.25. In order to calculate security quality, we let

$$q_1 = 1 - \frac{\#Customization\,Vulnerabilities}{Maximum\#Vulnerabilities} = 0.75.$$

In a similar way, for the Samsung Galaxy S3, 40 vulnerabilities were found, and 33 of these are the result of customization. Hence, we have $q_2 = 1 - \frac{33}{40} = 0.1750$.

Price: The prices of the HTC One X and the Samsung Galaxy S3 are equal to €170 [13] and €190 [14], respectively. GSM Arena (http://www.gsmarena.com/) groups both of these devices as group 4 out of 10 for their price. Here, we consider $p_1 = p_2 = 4$.

Parameter Estimation: By inserting these six values into our model analysis, we can calculate the six constants in our model. Here, we assume that both vendors are completely rational and as a result they have chosen their customization levels, prices, and security qualities following the dependencies captured by our model. Therefore, we can calculate the parameters in our model in a reverse way. By inserting our quantified parameters, i.e., a, b, q_1, q_2, p_1, and p_2, into Equations 8 and 9, we have two equations and two variables, i.e., β and T. The system of equations then yields the values of β and T. Note that these two equations are linear in T and β. Therefore, the resulting answer is unique.

To calculate the values of C_1, C_2, S_1, and S_2, we assume that the measured values of q_1, q_2, a, b form a Nash equilibrium of our game. Since the vendors' strategies are mutual best responses in a Nash equilibrium, q_1, q_2, a, b are solutions to the corresponding best-response equations, which are available in the extended version of the paper [7]. We have four variables and four equations. The solution of this system of equations provides the values of S_1, C_1, S_2, C_2, which are unique. Therefore, based on the measured values, we have $\beta = 0.4362$, $T = 5.7414$, $S_1 = 0.6723$, $C_1 = 1.4882$, $S_2 = 4.1338$, and $C_2 = 2.4875$.

6 Fine Model and Analysis

The background on actual security practices and our analysis provide evidence and explanations for vendors' unsatisfactory security practices in the context of customization. In particular, vendors will not adequately invest in security if consumers do not take security sufficiently into account. In the following, we propose a mechanism to incentivize a vendor to invest in security quality. In doing so, we introduce a regulator whose role is to define a corresponding policy. More specifically, we propose the following fine function for vendor i for a regulatory policy which takes as input the vendor's security quality and outputs the monetary value of the fine imposed on the vendor:

$$f_i(q_i) = \begin{cases} F\left(q^{min} - q_i\right) & \text{if } q^{min} \geq q_i \\ 0 & \text{otherwise,} \end{cases} \tag{12}$$

where F and q^{min} are constants defined by the regulator. q^{min} is the minimum acceptable level of security from the regulator's point of view and the regulator tries to force each vendor to satisfy at least this security level. F is a coefficient relating quality to monetary value and denotes the monetary value of fine for each unit of security violation from q^{min} for a vendor. The monetary value of the fine should be proportional to the market share, since a higher market share of a vendor with security issues results in a higher number of consumers with vulnerabilities. In our model, we multiplied f_i by the market share of that vendor.

In this section, we show that under certain conditions, a regulator can force a vendor to spend on security issues resulting from customization. Moreover, we prove that the product's price *decreases* as the vendor invests in the adequate level of security imposed by the regulator, for the same value of customization cost. More specifically, our analysis shows that under some conditions, the higher the security quality imposed by the regulator is, the lower the product's price is.

By imposing a fine, the vendors' utilities change to the following:

$$\pi_1 = p_1 D_1 - C_1 \left(a - Z_A\right)^2 - S_1 q_1^2 \left(a - Z_A\right)^2 - f_1 D_1. \tag{13}$$

$$\pi_2 = p_2 D_2 - C_2 \left(1 - b - Z_A\right)^2 - S_2 q_2^2 \left(1 - b - Z_A\right)^2 - f_2 D_2. \tag{14}$$

It is worth mentioning that the consumers' utility does not change. Hence, all of Equations 5, 6, and 7 are still valid for the case when there is a fine. The validity of these equations implies that the formulae for the vendors' market share is the same for both cases. However, the vendors' equilibrium prices are different compared to the previous case.

Similar to the case without a fine, here we have the same two stages with the same ordering. The regulator's goal is to force the vendors to invest in an adequate security level. Hence, in our analysis, we focus on the case where the regulator forces the vendor to invest in an adequate security quality level.

Theorem 2 characterizes both vendors' prices in Nash equilibrium when the regulator imposes a fine.

Theorem 2 *The Nash equilibrium in prices, which always exists, is*

$$p_1^* = \frac{\beta}{3}\left(q_1 - q_2\right) + T\left(1-a-b\right)\left(1 + \frac{a-b}{3}\right) + \frac{2f_1}{3} + \frac{f_2}{3}, \tag{15}$$

$$p_2^* = \frac{\beta}{3}\left(q_2 - q_1\right) + T\left(1-a-b\right)\left(1 + \frac{b-a}{3}\right) + \frac{2f_2}{3} + \frac{f_1}{3}. \tag{16}$$

This proof of the theorem is included in the extended version of the paper [7].

By comparing the above two equations with Equations 8 and 9, we observe that the introduction of a fine will increase the product price of the vendors for fixed locations and security level.

Naïve Consumers: Based on Theorem 2, by letting $\beta = 0$, we can characterize the price NE for naïve consumers (see the extended version of the paper [7]). Lemma 2 introduces the sufficient conditions to force vendors to invest in adequate level of security, when consumers do not take security into account.

Lemma 2 *Both vendors invest in $q_1^* = q_2^* = q^{min}$, if the following conditions are satisfied for the optimal locations of both vendors:*

$$F^2 - 18TS_1\left(1-a-b\right)\left(a - Z_A\right)^2 \geq 0, \tag{17}$$

$$F^2 - 18TS_2\left(1-a-b\right)\left(1-b - Z_A\right)^2 \geq 0, \tag{18}$$

$$3 + a - b - \frac{Fq^{min}}{T\left(1-a-b\right)} \geq 0. \tag{19}$$

Proof of the above lemma is provided in the extended version of the paper [7].

Lemma 3 calculates the location Nash equilibrium of both vendors considering that the regulator forces the vendors to invest in adequate levels of security.

Lemma 3 *For a given b, vendor 1's best response for location, when the consumers do not take security into account and conditions of Lemma 2 are satisfied, is as follows:*

• $C_1 + S_1\left(q^{min}\right)^2 \leq \frac{T}{12Z_A}$*: Vendor 1 differentiates its product the most, i.e., $a^*(b) = 0$.*

• $C_1 + S_1\left(q^{min}\right)^2 \geq \frac{T}{9Z_A}$*: The positive root of the following quadratic equation is called a_2. In this case, for vendor 1 we have $a^*(b) = \min\{a_2, Z_A\}$.*

$$-3Ta^2 + a\left(2Tb - 10T - 36\left(C_1 + S_1\left(q^{min}\right)^2\right)\right) + T\left(b^2 - 2b - 3\right) + 36\left(C_1 + S_1\left(q^{min}\right)^2\right)Z_A = 0 \quad (20)$$

- $\frac{T}{12Z_A} < C_1+S_1\left(q^{min}\right)^2 < \frac{T}{9Z_A}$ *and* $b \le \min\{1-\sqrt{4-\frac{36\left(C_1+S_1\left(q^{min}\right)^2\right)}{T}Z_A}, Z_A\}$: *Vendor 1 chooses its location as* $a^*(b) = \min\{a_2, Z_A\}$.
- $\frac{T}{12Z_A} < C_1+S_1\left(q^{min}\right)^2 < \frac{T}{9Z_A}$ *and* $1-\sqrt{4-\frac{36\left(C_1+S_1\left(q^{min}\right)^2\right)}{T}Z_A} \le Z_A$ *and* $1-\sqrt{4-\frac{36\left(C_1+S_1\left(q^{min}\right)^2\right)}{T}Z_A} \le b \le Z_A$: *Vendor 1 differentiates its product the most, i.e.,* $a^*(b) = 0$.

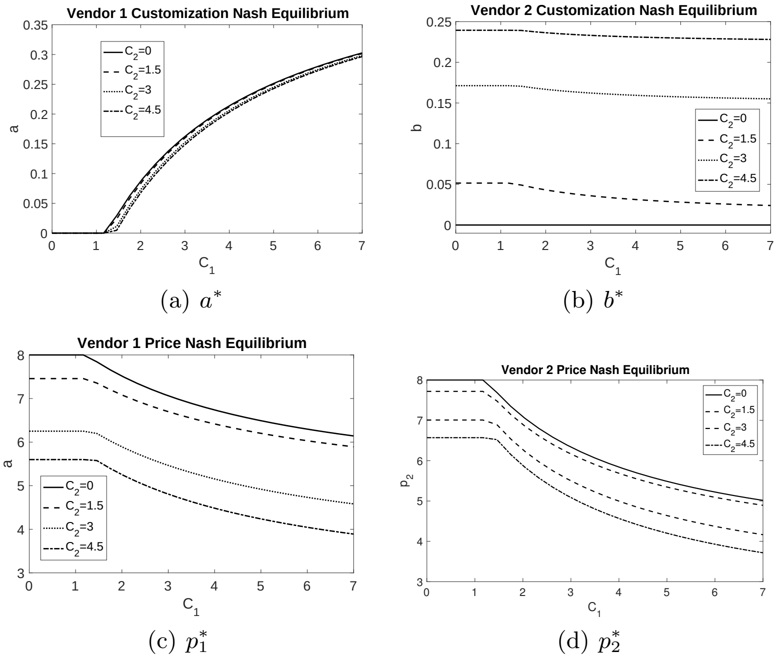
By changing C_1 to C_2, S_1 to S_2, a to b, and Z_A to $(1 - Z_A)$, in the above lemma, we can derive the same results for vendor 2. Proof of Lemma 3 is provided in the extended version of the paper [7].

Comparing Lemma 3 with the case without fine, maximal differentiation occurs when the customization cost is lower than when there is no fine, since a vendor's cost is affected by both the costs of customization and security quality. Further, according to Equation 20, the location NE depends on q^{min} rather than F. However, both F and q^{min} have the effect to satisfy the conditions for forcing a vendor to invest in an adequate level of security, i.e., Lemma 2.

7 Numerical Illustration

In this section, we evaluate our findings numerically. First, we evaluate the case in which consumers are naïve, but a regulator imposes fines. Then, we compare the equilibrium prices and locations in the absence and in the presence of the regulatory fine. Interestingly, we observe that the *products' prices* (of both vendors) *decrease* in the presence of fines, and both vendors invest in the minimum level of security q^{min} set by the regulator. Finally, we evaluate the case in which there are no fines but the consumers take into account security quality.

In Figure 2, we examine the effect of regulation on location, price, and security quality for various values of C_1 and C_2. In our evaluation, in the presence of a regulator, the conditions of Lemma 2 are satisfied. As a result, both vendors invest in q^{min} set by the regulator. Similar to the case without any fine, the higher the customization cost (e.g., C_1), the lower is the differentiation from the baseline AOSP (e.g., the higher the value of a^* is). Similarly, we again observe little changes in a vendor's location in response to changes in its opponent's customization cost and the customization level. Further, the equilibrium prices of both vendors are decreased by an increase in customization costs, since both of them choose lower levels of customization and enter a price competition. Note that even in the presence of fines, vendor 2 chooses the maximum level of customization (i.e., $b^* = 0$) when $C_2 = 0$, considering that its cost of security is



(a) a^*

(b) b^*

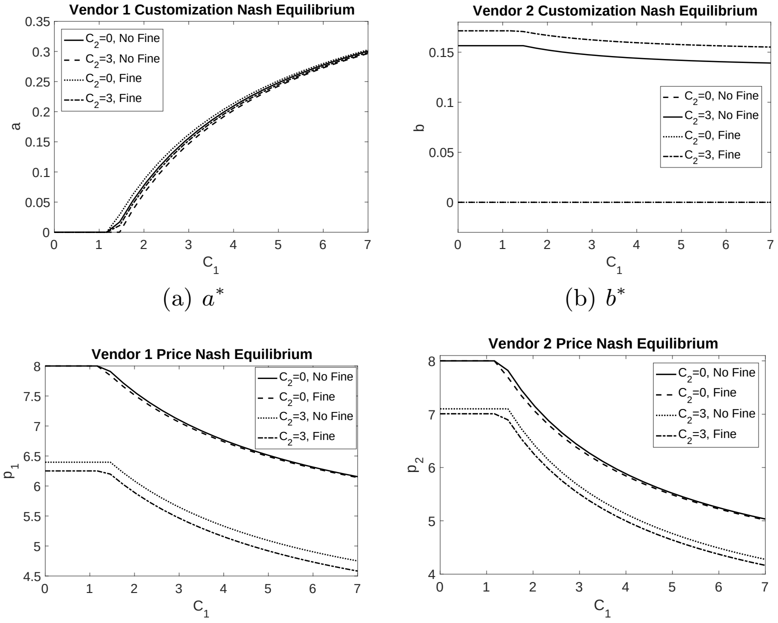
(c) p_1^*

(d) p_2^*

Fig. 2. Equilibrium locations and prices for various values of C_1 and C_2. Here, consumers are naïve, but there is a regulatory fine, and $T = 8$, $S_1 = 0.602$, $S_2 = 1.54$, $F = 10$, and $q^{min} = 0.4$. For these values of C_1 and C_2 and choices of a and b, both vendors invest in q^{min} set by the regulator.

proportional to its level of customization and $S_2 > S_1$. The reason for this is that vendor 2 is reluctant to enter a price competition.

In Figure 3, we compare the equilibria in the presence and the absence of a regulatory fine, when consumers do not take security into account. Based on Figure 3(c), vendor 1 chooses a lower level of customization when a fine exists. Figure 3(d) shows that vendor 2 chooses the same location in both cases as we discussed earlier when $C_2 = 0$. For $C_2 = 3$, vendor 2 chooses a lower level of customization (i.e., higher value of b^*) compared to the case when there is no fine. Consequently, the prices of both vendors are lower for higher customization costs due to the fact that both vendors are moving closer to the AOSP baseline model. Moreover, the existence of regulation and the fine leads to higher values of a^* and b^* (i.e., lower customization levels) for the same customization costs compared to the case without a fine, since each vendor tries to maximize its utility by avoiding a regulatory fine through investing in the minimum level of security quality q^{min}. Therefore, each vendor has to pay both the cost of customization as well as the cost of security quality resulting from customization. To decrease these costs, each vendor chooses a lower level of customization. Further, choosing higher values of a^* and b^* (i.e., lower customization level) leads to lower prices for both vendors. Therefore, the existence of a regulatory fine leads to **more**



(a) a^* (b) b^*

(c) p_1^* (d) p_2^*

Fig. 3. Comparison between the presence and the absence of a fine for naïve consumers. We have $T = 8$, $S_1 = 0.602$, $S_2 = 1.54$, $F = 10$, and $q^{min} = 0.4$.

secure products at **lower prices** when consumers cannot evaluate security properties by themselves.

To find equilibrium locations and security qualities when consumers take security into account but there is no fine, we calculate each vendor's best-response security quality and location for its opponent's given location and security quality. Then, the Nash equilibrium is the intersection of these best responses. Table 4 shows the equilibrium for various values of C_1, where $T = 1.6$, $\beta = 0.6$, $C_2 = 1.3$, $Q = 1$, and $S_1 = S_2 = 1$. In this case, due to the consumers' security considerations, both vendors invest in security. For $C_1 = 0$, vendor 1 maximizes its differentiation from baseline AOSP. Because of the consumers' security awareness, vendor 1 invests in security, but at a lower level than Q. It is interesting to see that vendor 2 does not differentiate its product from the baseline AOSP version due to maximal differentiation of vendor 1 and consequently, it does not have any security issues resulting from customization (i.e., $q_2^* = Q = 1$).

It is noteworthy that both vendors invest in the maximum level of security when both vendors' customization costs are greater than zero. This observation shows that if all consumers are capable of measuring security quality and it is one of the factors affecting their product choice, then vendors will invest in security. Similar to the case where consumers do not take security into account, the higher the customization cost, the lower is the customization level. In other words, increasing C_1 results in higher values of a^*. Moreover, changing the value of C_1, while C_2 is fixed, results in little changes in b^*.

C_1	a^*	q_1^*	b^*	q_2^*
0	0	0.2612	0.5	1
0.3684	0.2888	1	0.3639	1
0.7368	0.3195	1	0.3638	1
1.1053	0.3452	1	0.3637	1
1.4737	0.3677	1	0.3636	1

Table 4. The vendors' equilibrium prices and security qualities for various values of C_1. Here, we have $S_1 = S_2 = 1$, $T = 1.6$, $\beta = 0.6$, $Q = 1$, and $C_2 = 1.3$.

8 Conclusion

Our model shows that vendors have to invest in security quality for security-conscious consumers. Further, for naïve consumers, our proposed model captures the fact that vendors underinvest in security. To incentivize vendors to invest in security for naïve consumers, a regulator may assign a fine to those vendors that do not uphold a desired level of security, which is a well-motivated scenario given Android-related FTC actions [9].

We show that the imposed fine structure achieves the expected effect in addition to changes in the competitive landscape. First, the price of the product decreases for the same cost of customization compared to the case without any fine. Second, a higher level of security quality imposed by the regulator leads to a lower product price, if certain conditions are satisfied. Our findings suggest that requiring higher baseline levels of security investments (as triggered by recent FTC actions [9]) does not impose higher product prices on naïve consumers, which is important from a technology policy perspective. Moreover, increasing consumers' attention about security is substantiated by our analysis as a positive and meaningful factor to address challenges related to informational market power and neglected security efforts.

Acknowledgments: We thank the anonymous reviewers for their comments. The research activities of Jens Grossklags are supported by the German Institute for Trust and Safety on the Internet (DIVSI). Aron Laszka's work was supported in part by the National Science Foundation (CNS-1238959) and the Air Force Research Laboratory (FA 8750-14-2-0180).

References

1. Y. Aafer, X. Zhang, and W. Du, *Harvesting inconsistent security configurations in custom Android ROMs via differential analysis*, Usenix Security Symposium, 2016.
2. Android market share, *Android market share*, Available at: `http://www.idc.com/prodserv/smartphone-os-market-share.jsp`.
3. H. Beales, R. Craswell, and S. C. Salop, *The efficient regulation of consumer information*, The Journal of Law and Economics **24** (1981), no. 3, 491–539.
4. H. Cavusoglu and S. Raghunathan, *Selecting a customization strategy under competition: Mass customization, targeted mass customization, and product proliferation*, IEEE Transactions on Engineering Management **54** (2007), no. 1, 12–28.
5. C. d'Aspremont, J. Gabszewicz, and J.-F. Thisse, *On Hotelling's "Stability in competition"*, Econometrica **47** (1979), no. 5, 1145–1150.

6. R. Dewan, B. Jing, and A. Seidmann, *Product customization and price competition on the internet*, Management Science **49** (2003), no. 8, 1055–1070.
7. S. Farhang, A. Laszka, and J. Grossklags, *An economic study of the effect of Android platform fragmentation on security patch updates*, CoRR **abs/1707.06247** (2017).
8. Federal Trade Commission, *FTC to study mobile device industry's security update practices*, Available at: `https://www.ftc.gov/news-events/press-releases/2016/05/ftc-study-mobile-device-industrys-security-update-practices`.
9. ———, *HTC America settles FTC charges it failed to secure millions of mobile devices shipped to consumers*, Available at: `https://www.ftc.gov/news-events/press-releases/2013/02/htc-america-settles-ftc-charges-it-failed-secure-millions-mobile`.
10. A. Felt, E. Ha, S. Egelman, A. Haney, E. Chin, and D. Wagner, *Android permissions: User attention, comprehension, and behavior*, Symposium on Usable Privacy and Security, 2012, pp. 3:1–3:14.
11. J. Gabszewicz and J.-F. Thisse, *Price competition, quality and income disparities*, Journal of Economic Theory **20** (1979), no. 3, 340–359.
12. J. Galbraith, *The new industrial state*, Princeton University Press, 2015.
13. GSMarena, *HTC One X price*, Available at: `http://www.gsmarena.com/htc_one_x-4320.php`.
14. ———, *Samsung Galaxy S3 price*, Available at: `http://www.gsmarena.com/samsung_i9300_galaxy_s_iii-4238.php`.
15. D. Han, C. Zhang, X. Fan, A. Hindle, K. Wong, and E. Stroulia, *Understanding Android fragmentation with topic analysis of vendor-specific bugs*, 19th Working Conference on Reverse Engineering, 2012, pp. 83–92.
16. H. Hotelling, *Stability in competition*, The Economic Journal **39** (1929), no. 153, 41–57.
17. N. Kaldor, *The economic aspects of advertising*, The Review of Economic Studies **18** (1950), no. 1, 1–27.
18. F. Kardes, *Omission neglect*, Encyclopedia of Social Psychology (R. Baumeister and K. Vohs, eds.), vol. 1, Sage, 2007.
19. P. Mutchler, Y. Safaei, A. Doupé, and J. Mitchell, *Target fragmentation in Android apps*, IEEE Security and Privacy Workshops (SPW), 2016, pp. 204–213.
20. A. Mylonas, A. Kastania, and D. Gritzalis, *Delegate the smartphone user? Security awareness in smartphone platforms*, Computers & Security **34** (2013), 47–66.
21. S. Salop, *Monopolistic competition with outside goods*, The Bell Journal of Economics **10** (1979), no. 1, 141–156.
22. Singh, S., *An analysis of Android fragmentation*, Available at: `http://www.tech-thoughts.net/2012/03/analysis-of-android-fragmentation.html#.WA_OxoMrKUk`.
23. D. Thomas, A. Beresford, and A. Rice, *Security metrics for the Android ecosystem*, ACM CCS Workshop on Security and Privacy in Smartphones and Mobile Devices, 2015, pp. 87–98.
24. J. Tirole, *The theory of industrial organization*, MIT Press, 1988.
25. L. Wu, M. Grace, Y. Zhou, C. Wu, and X. Jiang, *The impact of vendor customizations on Android security*, ACM Conference on Computer & Communications Security, 2013, pp. 623–634.
26. X. Zhou, Y. Lee, N. Zhang, M. Naveed, and X. Wang, *The peril of fragmentation: Security hazards in Android device driver customizations*, IEEE Symposium on Security and Privacy, 2014, pp. 409–423.