Software Piracy Prevention through Digital Rights Management Systems

Petar Djekic & Claudia Loebbecke
University of Cologne, Dept. of Media Management
{petar.djekic | claudia.loebbecke}@uni-koeln.de

Abstract

Software publishers use Digital Rights Management, specifically copy-protection techniques, to prevent unauthorized and illegal copying of their software products. Common forms of prevention are copy-protection techniques based on physical tokens. While physical tokens provide better protection from unauthorized copying than intangible ones, the protected digital content becomes unsuitable for online distribution. This paper investigates the role of copy-protection techniques based on physical and intangible tokens in software piracy prevention. An internationally organized online survey among users of sequencer software, a particular kind of music software, provides the data for the subsequent descriptive analysis and logistic regression. Based on our findings, we present the general implications of our results for a software publisher's anti-piracy and online distribution policy.

1. Introduction

One reason why the potential cost advantages of online software distribution have not been fully exploited are the software publishers' concerns regarding illegal copying of their software products [2]. Online distribution does only allow for copy-protection techniques based on intangible tokens, which offer less protection from illegal copying than physical ones as these are harder to copy or generate. However, secure protection from illegal copying of application software, is a major concern for software publishers. According to the Business Software Alliance, software publishers lost USD 11 billion in 2002 due to illegal copying of their products, generally referred to as software piracy, with 39% of the world's software installations being illegal copies [3].

On the contrary, different authors [1, 7] point to a weakness in current copy-protection techniques based on intangible or physical tokens. Application software can be 'cracked', the checks for the token are removed from the application code, yet the software itself remains fully functional. While this weakness has been identified, the resulting effects on software piracy have not been empirically investigated.

In this context, this paper investigates the role of token-based copy-protection techniques as a preventive measure against software piracy. We choose sequencer software for our investigations as many different token-based copy-protection techniques are used for this type of application software, allowing us to analyze a broad range of protection approaches.

2. Copy-Protection Techniques

We distinguish into token-based and token-less copy-protection techniques. Common token-less copy-protection techniques are obfuscation, encryption, watermarking or fingerprinting [7, 15]. As these do not directly affect the ability to copy software, they are not taken into account in this study.

Token-based copy-protection techniques use an intangible or a physical token to protect the application software from illegal copying. They are the most common form of copy protection. The application software checks for the presence of the token and refuses to run until the token is present [2]. This process is also referred to as authorization.

Table 1 presents an overview of the token-based copy-protection techniques studied and the sequencer software that they protect:

Table 1. Protection Techniques Studied

Technique	Used in Sequencer Software ...
Serial Number	Cakewalk Sonar, Synapse Orion,
Challenge-Response	ImageLine Fruityloops, Mackie Tracktion
CD-ROM	MOTU Digital Performer, Propellerheads Reason
Dongle	Steinberg Cubase, Steinberg Nuendo, Apple Logic
Expansion Card	Digidesign ProTools

1530-1354/05 $20.00 © 2005 IEEE

The token-based copy-protection techniques are similar to those found in other application software like operating systems (e.g., Windows XP's *Challenge-Response*) or entertainment software (e.g., *CD-ROM* checks in games software).

3. Literature Review

Various copy-protection techniques [1, 2, 15] and strategies [6, 16] have been proposed for software piracy prevention. The degree of security of different copy-protection techniques has also been investigated [1, 7]. Gopal and Sanders [8] show that deterrent measures like legal punishment are more effective against software piracy than preventive measures like copy-protection techniques. Yet we lack research that empirically evaluates the success of different token-based copy-protection techniques for piracy prevention in a single study.

The reasons for software piracy and the user's 'pirate-or-buy' decision have also been studied extensively. Cheng et al. [4] as well as Gopal and Sanders [9] have identified economic issues as factors of software piracy, while Christensen and Eining [5] as well as Peace et al. [14] focus on psychological ones. Legal issues have been studied by Gopal and Sanders [8], and ethical by Kini et al. [11]. However, empirical research regarding the actual influence of technical factors, such as copy-protection techniques, on software piracy is rare.

4. Research Methodology

We assess the influence of the studied token-based copy-protection techniques (see Table 1) on software piracy in two steps.

First, we calculate the Piracy Rate for each token-based copy-protection technique. This allows us to assess the success of each protection approach in software piracy prevention. The Piracy Rate represents the percentage of sequencer software installations without license over all installations of sequencer software [3].

Second, we perform a binary logistic regression to estimate how each copy-protection technique affects the user's decision between installing legitimate or pirated sequencer software. We include an independent variable for each copy-protection presented in Table 1. In addition, we include the two independent variables 'Personal annual income', measured in US dollar, and 'Required for the workplace', measured as the share of the income earned from working with sequencer software. These two variables are included to assess the importance of each token-based copy-protection techniques in regard to these know two factors of software piracy [4, 9].

We used an online survey for data collection, which was split into two groups according to the form of invitation: email (Mail-Group) and posting to message-boards dealing with sequencer software (Board-Group). As the composition of both samples is different, the data of the Mail- and Board-Group is analyzed separately.

5. Research Results

The Mail-Group resulted in 219 completed questionnaires (7,99%). Email feedback indicated that the low response rate in this group was partially due to the cover letter being regarded as spam and outdated email addresses. In the Board-Group 575 questionnaires were filled out (26,63%).

Our data quality indicators are promising: The country of residence matched in 97% of the cases in the Mail-Group and in 93% of the cases in the Board-Group. The percentage of males and females in the Mail-Group (92% male, 8% female) and in the Board-Group (98% male, 2% female) are comparable to those of subscribers of the 'Electronic Musician' (89% male, 11% female).

5.1 Piracy Rates

The Piracy Rates (PR) for each copy-protection techniques are presented in Table 2.

Table 2. PR per Copy Protection Techniques (in %)

Techniques	MailG	BoardG
Serial Number	25	16
CD-ROM	24	30
Challenge-Response	50	23
Dongle	22	20
Expansion Card	7	9

5.2 Binary Logistic Regression

We use the following binary logistic regression model:

$$\ln[SI/1\text{-}SI]=\alpha+\beta_1\cdot SN+\beta_2\cdot C/R+\beta_3\cdot CDROM+\beta_4\cdot DONGLE+\beta_5\cdot EC+\beta_6\cdot WORK+\beta_7\cdot INCOME$$

with the independent variable *SN* measuring the influence of the copy-protection technique *Serial Number*, *C/R* the one of *Challenge-Response*, *CDROM* the one of *CD-ROM, Dongle* the one of *Dongle* and *EC* the one of *Expansion Card* on the probability of a legal or pirated sequencer software installation. *WORK* measures the influence of the independent variable 'Required for the workplace' and *INCOME* the one of 'Personal annual income'.

Table 3. Independent Variables – Mail-Group

Variable	β	Std. Err.	Sig.	Exp (b)
SN	-1,026	0,760	0,177	0,359
C/R	-3,252	1,498	0,030	0,039
CDROM	-1,647	0,491	0,001	0,193
DONGLE	-0,876	0,496	0,077	0,416
EC	-	-	-	-
WORK	0,296	0,115	0,010	1,345
INCOME	0,523	0,114	0,000	1,687

Table 4. Independent Variables – Board-Group

Variable	β	Std. Err.	Sig.	Exp (b)
SN	-0,165	0,528	0,754	0,848
C/R	-0,358	0,489	0,464	0,699
CDROM	-1,165	0,421	0,006	0,312
DONGLE	-0,455	0,417	0,276	0,635
EC	-	-	-	-
WORK	0,410	0,072	0,000	1,507
INCOME	0,599	0,197	0,000	1,821

According to Table 3 and 4, none of the variables related to copy-protection has a positive β-coefficients and is statistically significant (Sig. < 0,05). This means no protection increases the probability of a sequencer software installation being legal. The independent variable *EC* has been omitted in SPSS as the inclusion of this independent variable does not decrease the log-likelihood by more than 0,010%. Thus the inclusion of this variable would have not increased the explanatory power of the model. The *WORK* and *INCOME* variables increase the probability of a sequencer software installation being legal, since they both have positive β-coefficients and are statistically significant (Sig. < 0,05) in the Mail- and the Board-Group.

We assess the overall Model Fit with three Goodness-of-Fit tests (Table 5):

Table 5. Model Fit

	MailG	BoardG
LR-Test [10]	278,106 (Sig. 0,0)	758,684 (Sig. 0,0)
Hosmer-Lemeshow-Chi [10]	7,681 (Sig. 0,465)	17,663 (Sig. 0,024)
McFadden Pseudo-R^2 [12]	0,155	0,170
Nagelkerke Pseudo.-R^2 [13]	0,225	0,251

6. Major Findings

The Piracy Rates in Table 2 show that no token-based copy-protection techniques fully prevents unauthorized copying of the protected sequencer software in any of the groups, i.e., enforces a zero Piracy Rate. Moreover, all of the token-based copy-protection techniques have similar Piracy Rates, which indicates that implementing token-based copy-protection techniques has little effect on software piracy. The only exception is *Expansion Card*, which has Piracy Rates below 10% in both groups. Still, the results of our binary logistic regression show no significant influence of *Expansion Card* on the probability of a legal sequencer software installation, as with all the other token-based copy-protection techniques. Thus, the low piracy rates of *Expansion Card* are likely to be caused by other factors, e.g. the income structure of the protected software's users, rather than the technical protection itself. The values for our independent variables not related to protection, *INCOME* and *WORK*, are in line with previous research [4, 9]. The higher the personal annual income is and the more sequencer software is required for the workplace, the more likely is a legal sequencer software installation in both groups.

7. Study Limitations

Due to the characteristics of online surveys and the focus on users of sequencer software, our results cannot be easily generalized. Still, our findings may apply to software with similar user characteristics (e.g., Internet affinity) and token-based copy-protection techniques (e.g. CAD- or 3D-software).

The result of a logistic regression depends on the characteristics of the sample. A few outliers in the data or an unbalanced sample can lead to a bad model fit, resulting, for example, in a Pseudo-R^2 McFadden or Nagelkerke below 0,2. However, we could significantly improve the model fit only by including other factors of piracy as independent variables, such as software usage intensity [4]. As the model fit could be significantly increased only by additional variables, no removal of outlier datasets or ex-post balancing of the data was necessary.

8. Implications

Similar to the findings of Gopal and Sanders [8], our results show that a software publisher's anti-piracy policy should not only focus on preventive measures like token-based copy-protection techniques. The impact of personal income stresses the importance of adequate pricing strategies. This may not only include price differentiation by product features, but also by local market [9]. The independent variable 'Required for the workplace' shows that the likeliness of software piracy is partly dependent on the operational area of the application software. Software publishers could address these issues by implementing features, which make their products more useful for professional users. On the contrary, publishers of entertainment software are more exposed to software piracy and should take appropriate legal and pricing related measures.

Software publishers should not discard online distribution because they are not able to embed strong copy-protection techniques using physical tokens in their application software. Our results show that protection using physical tokens provides negligible advantages over protection using intangible ones in terms of software piracy prevention. By abandoning physical token-based copy-protection techniques software publishers are able to sell and deliver their product online, thereby reaching more potential customers than over traditional distribution channels.

9. References

[1] B. Anckaert, B. De Sutter, and K. De Bosschere, "Software piracy prevention through diversity", *Proceedings of the 4th ACM workshop on Digital Rights Management*, Washington DC, USA, November 2004, pp. 63-71.

[2] L. Atallah, and L. Jiangtao, "Enhanced Smart-card based License Management", *IEEE International Conference on E-Commerce*, June 2003, pp. 111-119.

[3] Business Software Alliance, "Annual Business Software Alliance Global Software Piracy Study", www.bsa.org/globalstudy/2003_GSPS.pdf, access on 02-10-2005, June 2003.

[4] K. Cheng, R. Sims, and H. Teegen, "To Purchase or to Pirate Software: An Empirical Study", *Journal of Management Information Systems*, 13(4), Spring 1997, pp. 49-60.

[5] A. Christensen, and M. Eining, M., "Factors Influencing Software Piracy: Implications for Accountants", *Journal of Information Systems*, 5(1), Spring 1991, pp. 67-80.

[6] K. Conner, and R. Rumelt, "Software Piracy: An Analysis of Protection Strategies", *Management Science*, 37(2), February 1991, pp. 125-139.

[7] P. Devanbu, and S. Stubblebine, "Software Engineering for Security: a Roadmap, *Proceedings of the International Conference on Software Engineering*, Limerick, Ireland, June 2000, pp. 227-239.

[8] R.D. Gopal, and G.L. Sanders, "Preventive and deterrent controls for software piracy", *Journal of Management Information Systems*, 13(4), Spring 1997, pp. 29-48.

[9] R.D. Gopal, and G.L. Sanders, "You can't get blood out of a turnip", *Communications of the ACM*, 43(9), September 2000, pp. 83-89.

[10] Hosmer, W., and Lemeshow, S., *Applied logistic regression*, Wiley&Sons, New York, USA, 2000.

[11] R. Kini, H. Ramakrishna, and B.S. Vijayaraman, "Shaping of Moral Intensity Regarding Software Piracy: A Comparison Between Thailand and U.S. Students", *Journal of Business Ethics*, 49(1), January 2004, pp. 91-104.

[12] D. McFadden, "The Measurement of Urban Travel Demand", *Journal of Public Economics*, 3(4), 1974, pp. 303-328.

[13] D. Nagelkerke, "A Note on a General Definition of the Coefficient of Determination", *Biometrika*, 78(3), 1991, pp. 691-693.

[14] G. Peace, D. Galletta, and L. Thong, "Software Piracy in the Workplace: A Model and Empirical Test", *Journal of Management Information Systems*, 20(1), Summer 2003, pp. 153-177.

[15] M. Peyravian, A. Roginsky, and N. Zunic, "Methods for preventing unauthorized software distribution", *Computers & Security*, 22(4), May 2003, pp. 316-321.

[16] O. Shy, and J.-F. Thisse, "A strategic approach to software protection", *Journal of Economics & Management Strategy*, 8(2), 1999, pp. 163-190.