Using the Internet to Reduce Software Piracy —
on Anonymous Receipts, Anonymous ID Cards, and Anonymous Vouchers

Author: Ralf C. Hauser, April 4, 1995
Presented by Quanzhong Li

1 Introduction

Copyright piracy occurs both on the producer side and the consumer side. The producer side experiences two forms of pirating:

1. Entirely illegal reproduction and distribution of pirated software and

2. The more subtle problem: authorized vendors defrauding their software publishers by for example interspersing illicit copies on their shelves which are not distinguishable from authentic packages by a buyer.

This paper discusses how a different software vending method supported by Internet technologies could alleviate the second problem.

2 Background and Assumptions

The primary assumption of the proposal is that honest users do not want to risk being prosecuted, without being guilty, because of software sold or installed on their hardware by infringing vendors against the terms of licensing contracts.

All involved parties (the honest users, vendors, and software publisher) are assumed to have Internet mail, PGP/PEM, MD5, and a certified public key. For the protection of privacy, anonymous re-mailers are assumed to exist to provide sender anonymity.
3 New Software Vending Method

When buying a software package in a store for $300, for example, the buyers only pay $30 for the material reproduction cost immediately, obtain a transaction number, and have to leave their address plus further assurances (e.g. ID card).

At home, the buyers verify the license terms by reading a LICENSE file. This file is signed by the software publisher and contains the publisher’s bank account number for the payment. The necessary public key certificate is retrieved over the Internet.

The buyers then pay the remaining $270 directly to the publisher, communicate the transaction number and obtain a receipt. The publisher then transfers a remaining amount of, for example, $40 to the vendor summing up to an adequate sales and profit margin. By bookkeeping the outstanding transaction numbers, the vendor knows which buyers need payment reminders.

This approach fulfills two goals: Honest users must no longer be afraid to unknowingly become victims of pirates and vendors have much less incentives to become pirates. As a standard of good practice, when purchasing, for example, the buyer will verify a permanent storage device, and the license terms of the software delivered with it. The mentioned misuse therefore can no longer occur unless a pirate vendor cooperates with a pirate consumer. This combination of criminal intents is contended to occur much more rarely than just an individual pirating.

4 Internet Support

With little extra effort, the relation between the software publisher and the buyers can be conditionally anonymized with ”Anonymous Receipts” obtained via electronic mail. The buyer sends with the payment also a number Y that is obtained by digesting: The user ID/address, the transaction number, a user chosen random number and further information (e.g. software serial number). The software publisher receiving the payment, not knowing the payer, signs a message containing: Y, date, product, and amount and returns it through anonymous mail.

If a buyer obtains a reminder from the vendor even though having paid, she or he will show this receipt. Only the buyer can authenticate the receipt by providing all components leading to Y. The random value is present to prevent the publisher from trying to rebuild Y over a potentially small buyer
5 Anonymous ID Card

The next step is to add conditional anonymity to the vendor-buyer relation. An anonymous ID card created in collaboration with a trusted notary will only reveal the buyer’s real ID in the case of unsuccessful payment reminders. The software distribution method can be further extended in a share-ware-like way. The honest buyers then obtain physical manuals and original disks by presenting ”Anonymous Vouchers” which they obtained over the Internet from the software publisher during the payment. Last, it is shown how also the purchase and delivery of software can be performed over the Internet securely employing the mentioned tools without the detour of physically going to potentially dishonest off-line vendors.

6 Bootstrapping Trust (TIOS)

Essential to all the mechanisms presented is that the honest consumer is capable of obtaining correct information enabling trustworthy verification of the software producer’s signature and policy data. This paper also proposes to use a Trusted Information Origin Server (TIOS) as a trusted third party of the copyright industry for this purpose.

7 Conclusion

This paper shows how piracy on the vendor or producer side can be reduced without unnecessarily undermine the privacy of consumers. Starting from a concrete scenario of a software sale, the anonymous receipts, ID cards, and vouchers can be employed in much more general scenarios. The paper has furthermore shown how these software sales can also be performed in a share-ware-like way, although assuming the relatively high trustworthiness of at least one of the consumers involved.

Last, the design of a trusted information origin server has been sketched. This service enables participants in global networks to comply fully with licensing terms without restricting current distribution methods, which may appear anarchic. If implementing the proposed software vending methods and consulting the TIOS becomes part of widely followed standards of good practice, the Internet may avoid becoming subject to rules such as government-imposed, rigid, compulsory license agreements, etc. that may
be cumbersome to follow and therefore detrimental to the future evolution of the network.