Computer Communications 82 (2016) 83–94

Contents lists available at ScienceDirect

Computer Communications

journal homepage: www.elsevier.com/locate/comcom

Privacy-aware loyalty programs

Alberto Blanco-Justicia, Josep Domingo-Ferrer*

Universitat Rovira i Virgili, UNESCO Chair in Data Privacy, Department of Computer Engineering and Mathematics, Av. Països Catalans 26, Tarragona E-43007, Catalonia

ARTICLE INFO

Article history:
Received 15 November 2014
Revised 27 November 2015
Accepted 13 February 2016
Available online 24 February 2016

Keywords:
Loyalty programs
Customer privacy
Anonymization
Blind signatures
Smartphones

ABSTRACT

Vendors use loyalty programs as a mechanism to incentivize returning customers, whose repeated transactions provide sustained profit and information on the customers' preferences. Such programs have become widespread, but they are facing criticism by business experts and consumer associations: since they facilitate profiling, a loss of consumer privacy ensues. We propose a protocol for privacy-aware loyalty programs that allows vendors and consumers to enjoy the benefits of loyalty (returning customers for the vendor and rewards for the consumers, respectively), while allowing consumers to stay anonymous and empowering them to decide how much of their profile they reveal to the vendor. The vendor must offer additional reward if he wants to learn more details on the consumer's profile. Our protocol is based on partially blind signatures and generalization of product receipts, and provides anonymity to consumers and their purchases, while still allowing negotiated consumer profiling. We provide empirical results that confirm the viability of our approach.

© 2016 Elsevier B.V. All rights reserved.

1. Introduction

Any vendor is extremely interested in establishing lasting relationships with consumers. For some companies (like public utilities or banks) long relationships are the rule rather than the exception, whereas for other companies (like retailers) consumer loyalty is much harder to obtain without specific incentives. Loyalty programs are instruments whereby vendors try to provide such incentives. In a loyalty program, the vendor pursues two main goals: (i) to encourage the consumer to make more purchases in the future (returning customer); (ii) to allow the vendor to profile the consumer in view of conducting market research and segmentation (profiled customer). In order to lure consumers into a loyalty program, the vendor offers them rewards, typically loyalty points that consumers can later exchange for discounts, gifts or other benefits offered by the vendor. Normally, enrollment to loyalty programs involves some kind of registration procedure, in which customers fill out a form with their personal information and are granted a loyalty card, be it a physical card (magnetic stripe or smartcard) or a smartphone application.

Market analysis and customer segmentation are carried out by building profiles of individual customers based on their personal information, which customers supply to the vendor during enrollment to the loyalty program, and their purchase records, collected every time customers present their loyalty cards. The profiles thus assembled are used in marketing actions, such as market studies and targeted advertising.

Although loyalty programs have become widespread, they are experiencing a loss of active participants and they have been criticized by business experts and consumer associations. Criticism is mainly due to privacy issues, because it is not always clear whether the benefits vendors offer in their loyalty programs are worth the loss of consumer privacy caused by profiling [1,16,25,32].

Loyalty programs can offer clear advantages to both vendors and consumers, like returning customers and special discounts, respectively. However, privacy concerns regarding buyer profiling affect more and more the acceptance of such programs, as the public awareness on the dangers of personal information disclosure is increasing.

In this work we propose a protocol for privacy-aware loyalty programs that allows vendors and consumers to enjoy the benefits of loyalty, while preserving the anonymity of consumers and empowering them to decide how accurately they reveal their profile to the vendor. In order to encourage customers not just to return but also to disclose more of their profile, the vendor must offer *additional* rewards to consumers. Thus, vendors *pay* consumers for their private information. On the other hand, consumers become aware of how much their personal data are worth to vendors, and they can decide to what extent they are ready to reveal such data in exchange for what benefits.

* Corresponding author. Tel.: +34977558109.
E-mail addresses: alberto.blanco@urv.cat (A. Blanco-Justicia), josep.domingo@urv.cat (J. Domingo-Ferrer).

http://dx.doi.org/10.1016/j.comcom.2016.02.002
0140-3664/© 2016 Elsevier B.V. All rights reserved.

To empower consumers as described above, we provide them with a mechanism that allows them to profile themselves, generalize their profiles and submit these generalized profiles to the vendor in an anonymous way. There are some technical challenges to be overcome:

- The proposed mechanism should prevent vendors from linking the generalized profiles to the identity of buyers, to particular transactions or to particular loyalty points submitted for redemption.
- To prevent straightforward profiling by the vendor, payment should be anonymous. In online stores, to completely achieve anonymity, the buyers should use some kind of anonymous payment system, such as Bitcoin [23], Zerocoin [22], some other form of electronic cash [13], or simply scratch cards with prepaid credit anonymously bought, say, at a newsstand. In physical stores, it would be enough to pay with cash.
- Consumers should not be able to leverage their anonymity to reveal forged profiles to the vendor, which would earn them rewards without actually revealing anything on their real purchase pattern.

Our proposed mechanism, thus, needs to take care of the two main aspects of loyalty programs. First, it has to provide a way to obtain and submit loyalty points in an anonymous and unlinkable way; that is, a customer should be able to submit a particular loyalty point to a vendor, but the vendor should not be able to link that particular loyalty point to the transaction in which it was issued. Second, our mechanism must allow customers to build their own generalized profiles from their respective purchase histories, but it must prevent customers from forging false profiles and vendors from linking the generalized profiles to particular customers. We will show later that these two aspects can be tackled in a similar way.

The paper is organized as follows. Section 2 starts recalling the functionalities of a conventional loyalty program; then it formalizes the notion of privacy-aware loyalty program; after that, it goes on to present the security and functionality requirements that our new privacy-aware protocol suite should satisfy. Section 3 reviews related work. Section 4 describes the cryptographic background used in our proposed construction, including bilinear maps, partially blind signatures, and zero-knowledge proofs. In Section 5, we explain how we use generalization of purchase receipts while preventing the existence of several generalizations of each purchase receipt from being abused to submit the receipt more than once to get loyalty points. In Section 6 we introduce anonymous tokens with controlled linkability based on partially blind signatures. In Section 7 we present our privacy-aware loyalty program protocol suite, that builds on the tools described in Sections 4, 5 and 6. In Section 8 we analyze the computational complexity and the security of the suite. In Section 9 we present experimental results, including an implementation on smartphones and an analysis of deployability in physical and online stores. Section 10 presents an extension of our construction that guarantees untransferability of purchase receipts and/or loyalty points. Finally, Section 11 summarizes conclusions.

A previous and partial version of this paper was presented in the conference paper [7]. Sections 3, 9 and 10 are entirely new to this journal version; also, substantial additions have been made to Section 2 (to which formalization and the untransferability requirement have been added), Section 4.2, Section 8 and Section 11. Furthermore, whereas [7] relied on symmetric pairings as the underlying cryptographic building block, we use here asymmetric pairings for increased security [14].

2. Loyalty programs

Our method aims to offer all the functionalities of loyalty programs; that is, to allow vendors to reward returning customers with loyalty points and to profile returning customers based on their purchase histories. The novelty is that our scheme empowers customers with the ability to decide how accurately they disclose their purchase histories to vendors.

A simple and perhaps the most widespread approach to implement a loyalty program is to have a centralized server, owned and operated by some vendor $\mathcal{V}$, that stores the information on the program participants. This information includes all the personal data the participants gave to the vendor when they enrolled to the program, their balance of loyalty points, and their history of purchases. Each customer is given a loyalty card which contains the identifier of her record in the server's database. Each time a customer buys at a store and presents her loyalty card, her record in the server is updated, by adding to it the items she bought and modifying her balance of loyalty points if needed. In this way, all transactions by each customer can be linked to each other using the customer's identifier. Even if the customer provided false information when she enrolled to the loyalty program, all of her transactions would be linked anyway. Hence, discovering the customer's identity in one individual transaction (*e.g.* through the credit or debit card used for payment) would allow linking her entire profile to her real identity.

If control over profiling and purchase histories is to be left to customers, a centralized approach does not seem a good solution. Moreover, we should also ensure that individual transactions cannot be linked to each other unless desired by the customer. To do so, we will let each customer manage locally and anonymously her own balance of loyalty points and history of purchases.

2.1. A privacy-aware alternative

Our proposed mechanism follows the decentralized approach. To allow local management of loyalty points and purchase receipts by the customer, we treat points and receipts as anonymous electronic cash, in the sense that: (i) they are one-time certified tokens of information; (ii) they are issued by vendors and they can only be redeemed at the same vendor who issued them, but issued tokens and redeemed tokens should remain unlinkable. However, unlike in anonymous electronic cash schemes, in our scheme the entity issuing certified tokens of information is not a trusted third party: indeed, the issuer in our scheme is the vendor, and placing complete trust in the vendor would allow him to profile the users. Moreover, the concrete implementation of the loyalty program should discourage customers from transferring loyalty points and purchase receipts among them. Purchase histories will be built by the vendor from the individual purchase receipts of all products purchased by each customer *that the customer allows the vendor to link together*; furthermore, the customer can decide how generalized/coarsened are the product descriptions in the purchase receipts she allows the vendor to link to one another.

Definition 1. (Privacy-aware Loyalty Program) A Privacy-aware Loyalty Program scheme has three participants: a key dealer or certification authority $\mathcal{CA}$, a vendor $\mathcal{V}$, and a customer $\mathcal{C}$. $\mathcal{V}$ keeps a set $\mathcal{DB}$ of submitted tokens that is initially empty. The scheme consists of seven protocols (Setup, VendorSetup, Enroll, Buy, Submit, Issue, Redeem):

- Setup is a probabilistic polynomial-time algorithm run by $\mathcal{CA}$ in which, on input a security parameter γ, outputs (and publishes) the system parameters params.

Download English Version:

https://daneshyari.com/en/article/449928

Download Persian Version:

https://daneshyari.com/article/449928

Daneshyari.com