An Advanced, Privacy-Friendly Loyalty System

Milica Milutinovic, Italo Dacosta, Andreas Put, Bart De Decker

An advanced, privacy-friendly loyalty system

Milica Milutinovic, Italo Dacosta, Andreas Put, and Bart De Decker

KU Leuven, Dept. of Computer Science, iMinds-DistriNet,
firstname.lastname@cs.kuleuven.be,
WWW home page: http://distrinet.cs.kuleuven.be/

Abstract. Loyalty systems are a very popular service employed by retailers in order to measure and reward customer loyalty. However, currently deployed systems introduce many privacy risks, as the users' data is completely controlled by retailers. In this work we tackle this issue by investigating the requirements posed on a privacy-friendly loyalty system and proposing a new design for a digital loyalty system. With this novel approach, the users are given more control over their data, but retailers are still able to measure their loyalty and perform (authorised) data collection. Additionally, the functionality of the design is flexible and allows for deployment of more advanced services.

Keywords: loyalty system, privacy, user profiles, anonymous credentials

1 Introduction

The retailing business has changed significantly over the last decades. The competitive environment has led to the development of new services that incentivise customer loyalty. Examples are the loyalty points system or personalised advertisement and offers. Although these approaches may increase user satisfaction, they also bring significant privacy concerns. In order to make personalised offers to the customers, or to reward their loyalty, the service providers simply record all their purchases. This data is then used to determine preferences or to measure customers' loyalty.

With this approach, users disclose information that is not required for delivering these services. Only a part of the revealed data would suffice to have fully featured services. When taking part in the aforementioned schemes, the customers are usually not aware of the magnitude of information that is collected or even how it will be handled. Data mining techniques are increasingly powerful and collected data can reveal much more than even privacy-wary users would suspect. Most importantly, these services do not require users' identities, but some providers nonetheless collect it. This provides a direct link between the behaviour and the identity of the customer. An additional concern is also the protection of the databases that store this data. Even with major providers, they can suffer from deliberate or accidental leakages [5].

Even though these services are becoming increasingly ubiquitous and privacy concerns are not negligible, little attention is given to developing solutions that

would protect the privacy of the users. Some providers shy away from employing these services, in order to avoid customers' negative reactions [16]. A recent survey indicates that almost 30% of customers believe that too much information is collected through the loyalty services, leading 24% of users to decline taking part in them [9]. This shows that a change in current practices is necessary.

Next to the aforementioned issues, an additional drawback of the existing systems is the practical aspect. With current deployment, the users are required to carry a physical card for every provider that offers a loyalty scheme. This can significantly affect user experience, taking into account the abundance of offered schemes. This is illustrated with a US survey suggesting that an average household is subscribed for 14 loyalty programs, while actively participating in almost half of them [3]. There are solutions, which offer simple transfer of loyalty cards to the smartphone [1, 2], but usability problems may arise as barcode detection and accuracy require multiple scanning attempts [4].

Contributions. In this work we tackle the aforementioned issues by designing a privacy-friendly loyalty system able to offer advanced services. We allow even privacy-concerned users to benefit from loyalty schemes by providing the means for them to control disclosure of their data. At the same time, service providers are still able to perform (authorised) data collection. To the best of our knowledge, this work also represents the first proposal in this area that explores using anonymous credentials technology for these services. By employing anonymous credentials on smartphones, the functionality of the design becomes more flexible and offers more advanced services, such as service providers collaboration or brand loyalty. This proposal aims to preserve the incentives for all the involved stakeholders - not only users, but also service providers. Additionally, by developing electronic loyalty cards that the users can carry and use with their smartphones, there is no longer the need for the users to carry a number of physical cards with them at all times.

Moreover, this work is applicable to users with different privacy preferences. Work of Hinz et al. [12] identifies three groups of users, classified according to their privacy concerns. The first group represents the users that are *privacy unconcerned* and are willing to reveal personal data even for small economic incentives offered by the provider. The second group are *pragmatic* users that do want to protect their privacy, but are willing to disclose portions of their personal information for the right rewards. The third group are users that are *privacy concerned* and are not willing to disclose personal information or participate in customer loyalty programs, regardless of the offered incentives. Our proposal is applicable to all three groups of users. Namely, the users can choose their level of anonymity and disclose selected information that would allow obtaining appropriate levels of incentives.

2 Related work

Privacy is recognised as an important concern in the loyalty schemes [13, 12]. However, there is not a significant body of research addressing this issue. Pro-

posals for improving privacy in the loyalty systems usually focus on unlinkability of the loyalty points issued to the user. In [14] the authors propose to have a batch of user loyalty cards available to users for anonymous download. While this allows the users to remain anonymous towards the system, the service provider cannot measure their loyalty, which imposes significant limitations and at the same time removes incentives of the retailers. A solution proposed by Enzmann and Schneider [10] uses blind signatures to avoid linking loyalty points in the issuing and the redeeming phase. Even though the users can collect loyalty points, there is no robust mechanism that prevents the users from sharing or merging their loyalty points. Additionally, in both approaches, there is no option for the retailer to record any data, even with user consent. Contrary to these proposals, we try to tackle the privacy issues of the loyalty systems, while preserving the incentives for all involved stakeholders. We also aim at providing new functionality, which is advantageous for the service providers, but also the customers.

The data that the loyalty systems collect about their users is also employed to personalise the delivered services. Those include personalised advertisements, offers and coupon issuance. While there is limited work on the topic of privacy in loyalty systems, there are related research proposals that try to tackle privacy-preserving personalisation of accompanying services. Work by Hardt and Nath [11] allows users to choose the amount of personal information that is to be disclosed to an ads server in order to be offered with personalised advertisement. The user sends (part of) her preferences to the ads server, which are used for coarse-grained filtering of ads that are sent to her. The user application then performs the final filtering of the received ads based on more detailed personal information. This way, the user is presented only with relevant advertisement and can still choose her level of privacy. A proposal of Partridge et al. [15] tries to solve personalised coupon delivery with user privacy protection. Namely, it uses locality sensitive hashing, allowing the server to send all coupons encrypted to a user, while she would only be able to decrypt the ones that are targeting her behaviour. Similarly to the described research efforts, our proposal allows to have the personalised services, while users have complete control over the level of data disclosure.

3 Loyalty system design requirements

We identify the following requirements that need to be achieved by a privacy-friendly loyalty system design. These requirements are also guiding the design decisions for the proposed system.

- *Unlinkability.* The design of the system should not allow the service provider to link different purchases of one user or to link purchases with user's personal information, without user's explicit authorisation.
- *Anonymity and selective disclosure.* Users of the loyalty system should be able to choose their level of anonymity. They may opt for remaining completely anonymous towards the provider, or may decide to disclose (a part of) their personal information.

– *Points unforgeability and double-spending prevention.* The users should not be able to create new points or reuse valid loyalty points.
– *No unauthorised points sharing.* The users should not be able to share or merge the loyalty points they obtain, unless they are authorised to do so (e.g. in a family loyalty scheme).
– *Flexibility.* The system design should be flexible to support different scenarios and different types of interaction between the user and the service provider.
– *Extensibility.* The design should allow ease of deployment of new services.
– *Deployability.* The proposed system design should not require any additional hardware at the user side which would impede system reception.
– *Compatibility.* The novel loyalty system should be compatible with the existing systems and be able to run in parallel.

4 Approach

The existing loyalty systems are based on sweeping user profiles maintained by service providers, which record all the personal information, loyalty information and shopping behaviour of users. When interacting with the store, the user only needs to authenticate by showing the loyalty card and disclosing the unique loyalty number. This number points to the profile of the user stored in the provider's database. The provider adds to the profile all the information from this latest interaction, such as the purchased items and obtained loyalty points. This, however, allows the service provider to record much more data than is actually needed for the service in question. Additionally, the authentication mechanism itself does not ensure that the user who is using the card is actually the user that was issued with it. In order to solve these issues, the approach of this proposal is to keep all user data on her device and disclose only chosen portions of it. At the same time, when authenticating, the users prove that they are legitimate system users and the loyalty tokens that are issued to her cannot be transferred to other entities without authorisation.

In order to provide such a privacy-preserving loyalty system design, we employ anonymous credentials technology. The loyalty card is issued to the user as an anonymous credential. It records their identifying data[1] and other information that is related to the service, such as the unique loyalty card number. As different usages of loyalty credential should not be linkable, we assume usage of Idemix credential technology [7]. In the interaction with the service provider, the user can choose which part of the data she wishes to disclose[2]. She may decide only to prove the fact that she is a legitimate user of the loyalty service offered by

[1] This information can remain hidden from the service provider throughout the card's lifespan. It can also be utilised if the user decides to disclose parts of it, but also prove the validity of the data.

[2] The system design assumes that the payment protocol protects user anonymity, i.e. the user does not disclose her identity or enable the service provider to link her purchases through the payment process, e.g. by using e-cash or involving an external payment service.

that service provider. The service provider thus maintains profiles with different levels of anonymity, but is ensured that the interacting customers are authorised loyalty system users.

As different levels of disclosure are possible, the users are incentivised to reveal more data by appropriate rewards, such as higher discounts or vouchers. The users may choose to only collect the default number of points and thus only prove that they possess a valid loyalty credential. The points are obtained independently and the user does not need to reveal their previous count. This is an additional improvement for the privacy, as it further reduces the possibility of making links between different user–provider interactions.

The second level of disclosure is allowing the provider to link the purchases the user makes. In this case, the user would reveal the unique loyalty number contained in the loyalty credential. This value is an attribute in the user's credential and therefore cannot be forged by other users. As an alternative, the provider can also be presented with a pseudonym based on the credential secret and some public value, allowing him to link the purchases in a pseudonymous profile. This way the user is able to reset her profile by changing her pseudonym.

Finally, privacy unconcerned users can disclose any data recorded in their credential, which the service provider is assured has been approved at the time of credential issuing.

4.1 Threat model.

The attacks to the loyalty system can originate from both internal and external attackers. Internal attackers can be legitimate users of the system, who may try to forge points, double-spend them or merge them without authorisation. Internal attacks can also be mounted by the retailer–or service provider–if he tries to obtain more data than the user authorises him to. On the other hand, an external attacker is an adversary who is not a legitimate participant in the loyalty scheme and who tries to defeat the system by attempting to use the loyalty system as a legitimate user without subscribing for it, and additionally forge loyalty points in order to obtain offered rewards.

4.2 Loyalty points.

Users can have a number of points issued to them. The points are linked to their anonymous credential and are not transferable. At the same time, the service provider does not have to acquire any unique data (e.g. identity or the unique loyalty card number). Additionally, with this approach, unauthorised points sharing or merging is prohibited. The users are not able to merge points linked to two different cards, i.e. anonymous credentials. Also, sharing the card would require sharing the credential itself, which is prohibited with existing credential sharing-disincentivising schemes. However, this approach still allows to offer *family cards* to the customers. That ensures that customers can still benefit from the family scheme, while not compromising their privacy. Each

family member is issued with a loyalty card which can be used independently, while the loyalty points are pooled together.

4.3 Advanced services.

With the proposed approach, new possibilities are opened, and new services can be developed within this system. As an example, the users can collect *brand-specific loyalty points* which are not retailer-specific. This allows the brand to incentivise and reward user loyalty directly. Also, different retailers can cooperate and loyalty obtained at one can be used to retrieve benefits with the other. For instance, users can be issued special points for all eco-friendly products they purchase and proving that they have obtained a certain number of points can allow them to gain benefits in an environmentally friendly store, or even with the government, which can offer certain incentives, such as specific tax reductions.

5 Cryptographic building blocks

This section provides an overview of the cryptographic building blocks used in the proposed system design.

- **Commitments.** Commitment schemes enable an entity to commit to a set of values while keeping them secret. These schemes are comparable to sealed, opaque envelopes. When a commitment is issued to a verifier, the user cannot change the values she committed to, without it being detectable by the verifier. The commitment hides the values chosen by the user, but still allows for proving certain properties of the committed values.
- **Blind signatures.** Blind signature are signing schemes that allow to hide the contents of a message when it is signed [8]. The concept is comparable to envelopes lined with carbon paper. The party that wishes some document to be signed by an authority, but still hidden from it, can enclose the document in such an envelope. The authority then signs the closed envelop and when the requesting party opens the envelope, it is presented with the signed document.
- **Zero-knowledge proofs of knowledge.** Proofs of knowledge in cryptography, are proofs in which one party, the prover, proves to a verifier that she holds certain knowledge [6]. With zero-knowledge proofs of knowledge, a prover can convince a verifier that a certain statement is true, without revealing any additional information.

6 Privacy-preserving protocols

In this section, we provide an overview of the protocols for issuing loyalty cards, obtaining and using loyalty points. We also present how to extend the offered services, without making any changes to the design of the system.

6.1 User registration

In order to participate in the loyalty scheme, the users initially need to register with a designated credential issuer in order obtain a loyalty credential. For user convenience, the protocol for issuing the anonymous credentials can also be performed through an online service. A standard protocol for issuing multi-show Idemix credentials [7] is used. The issuer can therefore be the provider itself, since the usage of the credential will not be linkable to the registration stage. In case of online issuance, interested users would initially contact and establish a secure connection with a trusted issuing party. They would possibly need to prove some personal information, such as identity, address and email address. For proving personal attributes, the electronic ID can be used, and other information, such as email or telephone number can be verified by the issuing party by simply sending a validation code to be returned. The user also chooses a random number to be included in her credential, but sends only a commitment to it, so that the issuing party cannot learn its value. The issuer applies a random offset to this value and the result represents loyalty card secret, which remains hidden from the issuer. The user is then issued with an anonymous credential which records her personal information, a loyalty credential number chosen by the issuer and the loyalty secret. The credential is stored and managed on the user's smartphone.

6.2 Obtaining loyalty points

When making a purchase and obtaining loyalty points, the user can choose her level of anonymity. In this work we describe the protocol in which the user remains completely anonymous towards the store, as the other levels of privacy can easily be derived from it. The only additional action that would be required from the user is to simply show or prove properties of attributes contained in her credential. Those can be the unique loyalty credential number or even her identity.

When a user makes a purchase and is to be awarded with a certain number of points, she initially creates a commitment to her loyalty secret, the number of points and the epoch that applies[3], and blinds this commitment. Using zero-knowledge proof of knowledge protocols, she proves that the blinded commitment is correctly created and that is contains the value from her credential. The store than verifies the proofs and checks that the correct epoch identifier and number of points are used. If these checks pass, the store signs this data and sends the signature to the user. The user then removes the blinding factor from the signature thus obtaining provider's signature on the commitment. The user finally stores the commitment and its opening information, number of earned points and the epoch together with the unblinded signature, which represents the points she has earned.

[3] The epoch number represents an indication of the period when the points were obtained. They are used, so that the service providers can limit the validity of the loyalty points.

In order to avoid any kind of linkability, the service provider should not issue unique numbers of points. With every purchase, the points can be divided into predefined amounts that are issued separately. This is an additional requirement that protects from the already limited possibility of service provider linking different purchases.

6.3 Using loyalty points

When a user wishes to redeem previously collected points in order to obtain certain benefits, the procedure is as follows. The user would give the store the collected signatures on the commitments, previously unblinded, along with the numbers of points they were mapped to and the epochs they were obtained in. The user also provides proof that the commitment is linked to her credential and that it is correctly created, using expected epoch and number of points. The store is then able to verify the applicability of the epochs in which the points were obtained and if the commitments were used before[4]. The store then verifies the validity of the signatures and the provided proofs. If all the checks are successful, the provider sums up all the points the user was issued with. It also stores the commitments and the corresponding epochs in order to detect and prevent double spending of the used points.

Optionally, these protocols can be simplified. It is possible is to omit the proof of having the loyalty secret in the user's credential. This step assures the store that the points are only spent by the user who obtained them. Therefore, in case points sharing is permitted, this step can be skipped.

6.4 Advanced services

Obtaining and using the loyalty points represent the basic functionality of the loyalty system. The designed protocols also allow for deployment of more advanced services, without introducing threats to user privacy.

Family loyalty card. The described scheme is applicable to family loyalty service. In order to merge the points they collect, family members only need to link their loyalty credentials at the time of issuing. One member initiates the process by choosing the random value for the creation of the loyalty secret and registers with the issuing party. At that point it is also required to specify how many family members will be participating in the loyalty scheme. After obtaining the credential with the loyalty secret created from the chosen random number with an offset applied by the issuer, the user distributes the chosen random number along with the loyalty number to the other members. They can then approach the issuing party, reveal the loyalty number they wish to have included in their credential, and obtain their loyalty cards, i.e. anonymous

[4] It checks the database where used commitments are stored together with their epochs. Once the epoch becomes invalid, the database can be cleared from the corresponding entries.

credentials with the same loyalty secret and loyalty card number included in them. The loyalty secret is the same for all the users, as the issuer stores and reuses the offset used for a specific card number. The issuer is able to verify that only the specified number of users obtains the credentials with the same loyalty number and loyalty secret.

In case of the family scheme, collection of points is performed in the same way as by the individual users. The collected signed commitments are stored in a joint cloud storage together with their opening information, so that a family member can merge and use them collectively. When the commitments are opened, any family member can successfully prove that they have been constructed as a function of an attribute contained in her credential.

Brand loyalty. The described scheme allows for brands loyalty, where the users would be issued loyalty points for purchases of specific brands' products. The only difference in the protocols is that the the brands identifier would be added to the commitment that is signed, similarly to the epoch identifier. The user is then able to prove that the points she was issued are linked with a specific brand giving her the appropriate benefits.

Privacy-preserving personalisation. The system can be easily extended to encompass personalised services. For instance, for personalised coupon delivery, the users can collect specific tokens when making purchases. The tokens would indicate the category of their interest and would be issued linked to the user's credential in a similar way as the loyalty points. When wanting to obtain personalised coupons, the user would prove that she was issued with a set of tokens, similar to showing the gathered points. This way the user can remain anonymous and her shopping behaviour would not be transparent to the provider or linkable to a profile, while the service provider can be ensured that the shown behaviour has not been fabricated or shared.

7 Discussion

This section discusses the protocols from the point of view of the requirements listed in Section 3.

- *Unlinkability.* When interacting with the service provider, the user by default does not disclose any unique or identifying information. For obtaining points, the user discloses only a blinded commitment to her loyalty secret. When the points are redeemed, the user shows the commitment itself, which cannot be linked to the initial blinded commitment.
- *Anonymity and selective disclosure.* By utilising anonymous credentials as loyalty cards, the users can choose their level of anonymity. No personal data from the credential is disclosed to the provider, unless the user explicitly authorises such an action.

– *Points unforgeability and double-spending prevention.* Since the users do not have the secret signing key of the provider, they cannot create valid signatures that would allow them to use points that are not authentic. They can also not reuse their obtained points, as the service provider checks for every received commitment whether it was seen before.
– *No unauthorised points sharing.* All the points that are issued are linked to the credential of the interacting user, and thus cannot be shared or merged amongst different users. It is however possible that users would lend the credential itself to another user, but that is less likely as the loyalty credentials are bounded to their smartphones, which also contain sensitive information. The loyalty credential sharing can also be prevented with existing schemes for disincentivising sharing.
– *Flexibility.* The system is applicable to different scenarios and can be utilised in both online and offline shopping.
– *Extensibility.* As described in the previous text, the design allows deployment of new services, such as brand loyalty or personalised coupon delivery.
– *Deployability.* No special hardware is required for the utilisation of the proposed system. The users can participate in the loyalty scheme with their smartphones.
– *Compatibility.* The loyalty system is compatible with the existing implementations and can run in parallel. The users that do not own a smartphone or are not privacy-concerned can continue using the plastic loyalty cards and have the service provider maintain their data and loyalty points.

8 Concluding remarks

This paper describes an enhanced loyalty system that provides benefits to providers while respecting user privacy. It also represents the novel approach for employing anonymous credentials technology in the loyalty systems design. Defense against described attacker models is provided by the properties of anonymous credentials. The customers are able to prove that they are subscribers of the loyalty system and choose the data they want to disclose. They are also ensured that the service provider has learned nothing more. Additionally, unauthorised parties cannot create valid credentials and the service provider is assured that he is interacting with legitimate users.

Both service providers and users benefit from the proposed design. Even the most privacy-concerned customers can use the system as they can choose the level of information disclosure. Optionally, they can collect points completely anonymously, even without the possibility of the provider linking different purchases. The service providers are able to perform authorised data collection, contrary to existing proposals. Such a system offers competitive advantage, as users are more enticed to select an option that ensures their privacy. Furthermore, this proposal provides new functionality, such as brand loyalty, i.e. brands themselves can measure and reward user loyalty, or privacy-preserving personalisation of loyalty services.

Acknowledgements

This research was funded by the IWT-SBO Project MobCom (A Mobile Companion).

References

1. Cardstar. http://www.cardstar.com/.
2. FidMe. http://www.fidme.com/en/home.html.
3. Getting a Business Lift from Loyalty program. Facts and Statistics. http://www.loyaltyleaders.org/facts.php.
4. http://gadgetwise.blogs.nytimes.com/2010/10/15/cardstars-vision-problem/.
5. Sony PlayStation data breach. https://www.privacyrights.org/data-breach-asc?title=Sony.
6. Mihir Bellare and Oded Goldreich. On defining proofs of knowledge. In *Proceedings of the 12th Annual International Cryptology Conference on Advances in Cryptology*, CRYPTO '92.
7. Jan Camenisch and Anna Lysyanskaya. An efficient system for non-transferable anonymous credentials with optional anonymity revocation. *Advances in CryptologyEUROCRYPT 2001*, 2045(2001/019):93118, 2001.
8. David Chaum. Blind signatures for untraceable payments. In *CRYPTO*, pages 199–203, 1982.
9. eMarketer. To keep users happy, loyalty programs must walk a fine line. http://www.emarketer.com/Articles/Print.aspx?R=1009958.
10. Matthias Enzmann and Markus Schneider. A privacy-friendly loyalty system for electronic marketplaces. In *e-Technology, e-Commerce and e-Service, 2004. EEE '04. 2004 IEEE International Conference on*, pages 385 – 393, march 2004.
11. Michaela Hardt and Suman Nath. Privacy-aware personalization for mobile advertising. In *Proceedings of the 2012 ACM conference on Computer and communications security*, CCS '12, pages 662–673, 2012.
12. Oliver Hinz, Eva Gerstmeier, Omid Tafreschi, Matthias Enzmann, and Markus Schneider. Customer loyalty programs and privacy concerns. In *Proceedings of BLED 2007*, 2007.
13. Il horn Hann, Kai lung Hui, Tom S. Lee, and I. P. L. Png. Consumer privacy and marketing avoidance. In *Equilibrium Analysis: Essays in Honor of*. Cambridge University Press, 2005.
14. Philip Marquardt, David Dagon, and Patrick Traynor. Impeding individual user profiling in shopper loyalty programs. In *Proceedings of the 15th international conference on Financial Cryptography and Data Security*, FC'11, pages 93–101, Berlin, Heidelberg, 2012. Springer-Verlag.
15. Kurt Partridge, Manas A. Pathak, Ersin Uzun, and Cong Wang. Picoda: Privacy-preserving smart coupon delivery architecture. 5th Workshop on Hot Topics in Privacy Enhancing Technologies (HotPETs 2012), pages 94–108, 2012.
16. Stefan Sackmann and Jens Strüker. *Electronic Commerce Enquête 2005: 10 Jahre Electronic Commerce - Eine stille Revolution in deutschen Unternehmen*. Konradin IT-Verlag, 2005.