A Lightweight Protocol for the Generation and Distribution of Secure E-coupons

Carlo Blundo
Dipartimento di Informatica ed Applicazioni
Università di Salerno
84081 Baronissi (SA), Italy
carblu@dia.unisa.it

Stelvio Cimato
Dipartimento di Informatica ed Applicazioni
Università di Salerno
84081 Baronissi (SA), Italy
cimato@dia.unisa.it

Annalisa De Bonis
Dipartimento di Informatica ed Applicazioni
Università di Salerno
84081 Baronissi (SA), Italy
debonis@dia.unisa.it

ABSTRACT

A form of advertisement which is becoming very popular on the web is based on electronic coupon (e-coupon) distribution. E-coupons are the digital analogue of paper coupons which are used to provide customers with discounts or gift in order to incentive the purchase of some products. Nowadays, the potential of digital coupons has not been fully exploited on the web. This is mostly due to the lack of "efficient" techniques to handle the generation and distribution of e-coupons. In this paper we discuss models and protocols for e-coupons satisfying a number of security requirements. Our protocol is lightweight and preserves the privacy of the users, since it does not require any registration phase.

Categories and Subject Descriptors

K.4.4 [**Computers and Society**]: Electronic Commerce—*Distributed commercial transactions, Security*; J.1 [**Computer Applications**]: Administrative Data Processing; K.6.5 [**Management of Computing and Information Systems**]: Security and Protection—*Authentication*; D.4.6 [**Operating Systems**]: Security and Protection—*Cryptographic controls, Authentication*; H.3.4 [**Information Storage and Retrieval**]: Systems and Software—*User profiles and alert services*; H.3.5 [**Information Storage and Retrieval**]: Online Information Services—*Web-based services, Commercial services*

General Terms

Design, Security, Verification

Keywords

E-commerce, e-coupons, security, accountability

WWW2002, May 7–11, 2002, Honolulu, Hawaii, USA.
ACM 1-58113-449-5/02/0005.

1. INTRODUCTION

The spreading diffusion of the Internet is causing a shift of traditional business processes from the real to the digital world. The role played by the Internet is that of a new powerful communication channel where it is possible to create new forms of business exploiting the opportunities deriving from the underlying technology. However, the transition from the real to the electronic world opens some problems and hides some difficulties that have to be correctly faced.

An example comes from electronic form of payments. In spite of the proliferation of e-commerce applications on the Internet, the most diffused payment mechanism for online transactions is still based on credit card number exchange. Such payments are very insecure and open the users to many risks exposing their credit card number during the communication with the server or when stored on the merchant's web site. Numerous fraud attempts have been registered in the past and even if several alternative forms of payments have been proposed, at the moment, the credit card system is the most requested way to finalize online transactions.

The same happens also in the field of online advertising. Indeed, Internet is more and more used to reach more and different customers and to influence their buying behavior. Merchants buy portions of a web page in the same way they choose space on a newspaper or a TV channel, selecting the most visited sites to get in touch with the largest number of people. Electronic advertising campaigns offer a rich potential to invent new forms of business and new strategies of communications to contact potential customers. Animated banners, interactive games and other kinds of promotions have been recently invented. On the other side, these techniques pose some problems related to the difficulty to measure the impact of an electronic advertisement campaign. Indeed traditional means to rate the success of advertisement campaigns, usually based on statistics, do not apply well to online advertisements where the number of users and the

differences among them are very high. *Metering schemes* [6, 13, 4] have been introduced as alternative systems to measure the exposure of online advertisements.

Coupons are one of the most diffused form of advertising and play a particular role, since they are contemporarily an alternative form of payment for part of the product value. They provide customers with discounts or gifts on the purchase of some merchandise and represent a very efficient tool to promote a particular product. In the USA, their distribution passed different phases, with a distribution rate ranging from 16 billion in 1970 to 310 billion in the peak year of 1992 (according to the data reported from the Grocery Manufacturers of America [11]). Although coupons are one of the most diffused forms of sales promotions, they suffer from a number of problems. First, the traditional distribution channels are relatively slow and present long lead times. Second, it is very difficult to finalize targeting strategy in order to select the potential customers interested in the particular promotion. Finally, since coupons must be saved and then used at the purchase, the redemption rates are quite low and unpredictable. To overcome these disadvantages, recently the Internet has become a distribution medium for traditional coupons [14, 15, 16]. A number of Web sites offers online coupons, in form of images or bar codes, which the customers have to print and then redeem at a particular physical store.

Shifting the concept of physical coupon used during the interaction between customer and merchant at a store, recently the concept of e-coupon has been introduced [10]. E-coupons are the electronic version of the real-world coupons which can be redeemed at online stores during e-commerce transactions. While the Internet offers marketing opportunities for the manufacturers and the retailers, using the Internet to distribute coupons has some inherent risks. Indeed, the digital nature of electronic coupons makes them prone to various kinds of frauds and security concerns are the primarily motivations which makes a number of manufacturers reluctant to adopt e-coupons [11].

Since coupons allow customers to buy some product at a reduced prize, they hide a monetary value too and many of the concerns related to electronic payment systems apply to the e-coupon generation and distribution systems as well. Differently from banners which can be considered advertising images with no value, the summation of the value of e-coupons can be considerably large: the 268,5 billion coupons distributed in 1996 in America, amount to 179 billion of dollars [11]. In this perspective, systems for the handling of e-coupons could be assimilated to e-cash system, where e-coupons are coins which are distributed by the issuers and spent by the customers at the moment of the purchase. However e-coupons, which can hold small or large monetary value, are usually bound to a single product, or a group of products or a particular manufacturer, showing then different usage patterns from e-money and requiring different protocols for their secure handling. Recently electronic coupon protocols have been presented, relying on signature schemes and digital certificates. Jakobbson et al. in [10] designed e-coupons as text messages which are digitally signed by the merchant who issues them. Other proposals adopt a centralized issuer acting as a coupon mint relying on a group signature scheme for the e-coupon distribution [7].

Our work presents the design of a lightweight electronic coupon protocol making e-coupons efficiently usable in e-commerce applications. The requirements of efficiency is particularly to be taken into account since protocols which require large computational resources are not practically usable. Potential customers can be discouraged if the time or the cost to download and redeem an e-coupon is comparable to the discount received. Different from previously proposed protocols relying on digital signature schemes and public key infrastructures [7, 10, 1, 2], our solution is based on MAC functions which can be more efficiently implemented. We discuss several models for e-coupons comprising a number of characteristics for the design of static and dynamic coupons (coupons whose value changes over time) extending the work in [5]. Our proposal respects consumers' privacy by avoiding the disclosure of personal data for the usage of valid e-coupons and is based on the provision of a unique identifier for each coupon in order to prevent double spending. Furthermore we discuss alternative pattern of usage for e-coupons resembling the mechanisms ruling their use in the real world and introduce other similar forms of promotions, such as purchase proofs.

2. THE SCENARIO

The scenario concerning the distribution of coupons involves different entities:

- **Manufacturers:** producers of goods who are willing to advertise their own products by stipulating a coupon-based advertisement contract with the advertisers;
- **Retailers:** the owners of the shops selling the promoted products. The consumers buy the promoted products at their online store eventually asking for the discount printed on their coupons;
- **Customers:** the clients buying the products at the merchant's or retailer's online store. Before buying a product the consumers collect the coupons related to that product in order to get a discount;
- **Advertisers:** people who agree with the manufacturer for an online advertising campaign based on the distribution of e-coupons to interested customers.

Different models have to be created according to the role played by the different entities. In particular it is

important to focus on the emitting authority and the redemption entity for e-coupons. Generation and redemption are the most delicate phases in the whole protocol and several security properties of the protocol depend on which entities play that roles.

2.1 The Basic Model

The simplest model is the one where the merchant is contemporarily issuer and redeemer. In this case the e-coupons are created and redeemed from the same authority. So the task to control the correct distribution and the validity of the presented coupon is easy.

The model is complicated by the introduction of the advertiser's role. Manufacturers own a web site and are able to finalize e-commerce transactions. To augment their business volume they can decide to stipulate a contract with one or more advertising agencies who own a web site or can rent web space on very popular web pages such that banners containing the manufacturer's offer can be displayed. This contract settles the terms of the advertisement campaign, including the specification of the e-coupon promotion. Indeed, the manufacturer should instruct the advertiser on the products she would like to promote, the amount of discount to be offered, the eventual conditions of the e-coupon's redemption, and other particulars of the promotion. The advertisers authorized by a manufacturer to release e-coupons on her behalf have to generate e-coupons according to the manufacturer's specifications.

Customers visiting the advertiser's web site can download the e-coupons there published. Users wanting to benefit from the offer will present the e-coupon for redemption to the manufacturer. The latter ones can obtain information on the success of their advertisement campaigns from the number of e-coupons redeemed by customers. In this way they can check also whether the amount of money paid to each advertiser to host their ads is worthwhile.

2.2 The Extended Model

In this section we extend the proposed model, including retailers as participants to the e-coupon exchange protocol. The emitting authority is still the advertiser who previously agreed with a manufacturer. However the e-coupons are no more directly redeemed at the manufacturer's web site but customers can spend them at a retailer's store, similarly to what happens in the real world. The role of the retailers is then to eventually accept the coupons the customers own and successively claim the corresponding amount of money to the manufacturer's site.

The distinction between the redemption, done by the customers, and the clearing, done by the retailers, opens some problems, since the retailers should accept an e-coupon and give the discount only if they are sure about the validity of the coupon. In this setting, the problem of double spending becomes heavier, since a malicious customer can duplicate and use the same coupon at different retailers. Furthermore dishonest retailers can collect and duplicate such coupons and blame customers for double spending. Other dishonest retailers could request the clearing to the manufacturer for coupons which have been not really used for the purchase of a product. To avoid this kind of problem a number of countermeasures have to be undertaken.

3. MODELING COUPONS TYPES

Different kinds of coupons are being currently used in practice. An electronic system should be able to emit the wide variety of e-coupon types resembling the mechanisms and the patterns of usage in the real world. Furthermore, it is possible to create new categories of e-coupons exploiting their digital nature. It is possible for example to create dynamic coupons, whose value changes over time according to determined parameters.

Coupons can be emitted by different authorities with different marketing purposes. *Manufacturer* coupons are issued by manufacturers of national brands to gain market share by persuading customers to switch to the promoted brand. This pattern of usage is typical when a new product is released to the market. Other popular goals of manufacturer coupons are to increase the sales of an existing product or to increase the re-purchase rate among occasional users of a brand. *Store* coupons are distributed by a particular physical store with different purposes: to attract new customers by discounting selected few products; to manage or reduce inventory or to reward customers loyalty.

As discussed in the previous section, in the handling of e-coupons it is important to determine the redeemer authority. If the issuer and the redeemer are the same entity, the handling of the e-coupons during the different phases of the protocol is easier. So the distinction between manufacturer and store coupons is no more useful in the online setting. A more useful distinction is between *static* e-coupons and *dynamic* e-coupons.

Static e-coupons resemble paper coupons which are distributed by magazines, whereas dynamic e-coupons introduce new features which are particularly useful in the context of electronic commerce. Static e-coupons usually hold a fixed discount and can be used within a fixed time which constitutes their validity period. It might be even the case that their value would change, for example, decrease, during this period but, as for their paper counterpart, there is no mean to determine the exact time when the user has obtained them.

Dynamic e-coupons contain information on the time when they have been downloaded by the user. They push the users to purchase the advertised merchandise as soon as possible by offering a discount whose value starts decreasing from the moment they are downloaded. Indeed, people who buy goods on the web are used to visit a large number of e-commerce sites in order to purchase the mer-

chandise at the most convenient price. Manufacturers who adopt dynamic coupons obtain duplex advantages: they discourage customers from shopping around in order to find a better priced product, and at the same time, they can get an immediate feedback of the success of their advertising campaign.

3.1 Purchase Proofs

Another advertising system which is currently in practice is the one in which the manufacturer releases a purchase proof after a customer has concluded a transaction. The purchase proof can be successively reused by the customer at the moment of another purchase, obtaining the gift or the discount which is associated to the proof. In the real world, the customer has to clip the tag which is attached on the product package and to carry it at a physical store to subscribe the offer.

In the digital scenario to resemble the mechanism above described, we assume that each product has an unique identifier, and that the purchase proof is released by the seller of the product during an online transaction. The customer will store the bit string holding the necessary data and reuse it at the moment of a successive purchase to get the associated discount. In the basic model, it is easy for the manufacturer to create the digital proof of purchase and to control it whenever the customer is willing to subscribe the offer. In the extended model, the store must have the capability to control the purchase proof presented by the customers and must associate it with the current transaction. In this case, the manufacturer and the retailer are protected against attempts to reuse the purchase proof and to avoid that retailers could claim the discount for purchase proof of not yet sold products.

Many of the following discussions apply to the generation and distribution of purchase proofs as well, but we do not enter into detail due to space limitations, remanding the interested reader to a future extended version of the paper.

4. REQUIREMENTS

In the following we will discuss the requirements a system for handling e-coupons should satisfy. The first three requirements concur in making the system lightweight.

Efficiency. The system must not require too much complex additional structures or computational resources; otherwise the overall cost of the advertising campaign could be exceeded by the costs necessary to set up the technical infrastructure.

Ease of use. The infrastructure for the coupon handling system should be easily deployable from both customers and manufacturers. Particular care has to be taken in the downloading and redemption phases; an excessive overhead could discourage customers to subscribe the offer.

Interoperability. The proposed system should reduce as far as possible the changes to the usual client-server communication pattern over the Internet. A manufacturer willing to set up an advertising campaign should not be compelled to make too many modifications to its site.

Customer's Anonymity. The privacy of the customers should be preserved, that is, customers should be able to download and redeem e-coupons without revealing any information about their identities.

Soundness. If all parties involved behave correctly, the system should allow manufacturers to have advertisers (resp., retailers) release e-coupons according to their specification, advertisers (resp., retailers) to issue e-coupons through their web sites, and customers to redeem e-coupons downloaded from the advertisers' (resp., retailers) web sites.

Observe that in stating the above property we have assumed that all parties involved behave according to the rules. Indeed, in a real-world scenario one has to contemplate the possibility that the parties involved in the system would cheat. Manufacturers are those who invest money in the system in order to receive some benefit in terms of publicity of their products. Manufacturers have no interest in breaking the system rules since any cheating attempt would discredit their promotional campaign. Hence, we can assume that manufacturers behave honestly and require the system to protect them from cheating attempts made by advertisers and customers.

4.1 Security Requirements

As reported in the GMA report [11], the security concerns are the motivations which make manufacturers reluctant to adopt e-coupons. Indeed, the digital nature of this kind of coupons makes them vulnerable to new kinds of frauds introducing thus a number of security issues.

Customers are interested in fooling the manufacturers in order to benefit of a more valuable offer than that provided by the downloaded e-coupons. To this aim they might either manipulate or duplicate e-coupons. On the other hand, the advertisers might release e-coupons which do not respect the merchant specifications to advantage particular customers. There are several reasons for doing this: either because the advertisers can be friends or even partners of the customers or because the advertisers want to make the e-coupons hosted by their web sites more appealing for the customers in order to attract a greater number of visitors. Further, a dishonest advertiser might not respect the manufacturers' specification in order to discredit their advertisement campaign. In particular the system should provide the following security requirements.

Protection from unauthorized issuance of e-coupons. Suppose that manufacturer M_i wants to start a promo-

tional campaign based on e-coupons distribution. To this aim she selects some of advertisers $A_1, \ldots, A_m$ and stipulates a contract with them. Obviously, M_i should be able to detect whether an e-coupon has been issued by an entity other than the authorized advertisers. We will refer to such illegal e-coupons as *fake* e-coupons. There are several situations where people can be motivated to generate fake e-coupons. As an example, consider the case when M_i hires the advertisers to release e-coupons only for a limited period of time but the promotional offer continues after that period. Then, a customer who has not been able to download the e-coupon from the advertiser web site may try to generate a fake e-coupon.

Fake e-coupons cause several drawbacks to the promotional campaign. They can damage the advertisement impact of the promotion since they are obtained without visiting the advertisers' web page. Furthermore, they can determine a notable economic loss for the manufacturer.

Protection from e-coupon manipulation. A manufacturer should be able to detect whether the e-coupon significant data have been altered. For example, a dishonest customer might manipulate the e-coupon to benefit of a better offer or to extend the validity period of the offer. On the other hand, a dishonest advertiser might alter the e-coupon issued by another advertiser so that it will appear as it was released by her.

Protection from e-coupon double spending. The system should protect the manufacturer from attempts by customers of redeeming the same e-coupon more than once. This eventuality is very likely to occur due to the fact that the e-coupons are digital data and consequently are very easy to duplicate.

In the dynamic setting the system should also provide the following security requirement.

Protection from postdated e-coupons. In the dynamic setting the emission date might be altered by the advertiser to advantage a particular customer who receives the e-coupon (they cooperate to fool the manufacturer). Indeed, a customer who receives a postdated e-coupon can delay the purchase of the promoted good and look for a better priced offer.

4.2 The Extended Model

A system for the extended model should verify all the requirements described in the previous section. Moreover, in the extended model the system should protect the manufacturers from attempts made by retailers to be paid back for more e-coupons than those which have been actually redeemed at their stores. For that reason, we want our system to satisfy the following additional requirement.

Protection from unredeemed e-coupons. A dishonest retailer might collect unredeemed e-coupons by downloading them from the advertisers' web sites, by secretly duplicating e-coupons presented by customers before redeeming them, or by generating fake e-coupons. Since retailers are reimbursed by manufacturers for each e-coupon which has been redeemed at their store, they can pretend that the e-coupons collected in this way have been redeemed at their stores and ask the manufacturers for reimbursement. For that reason, the system should allow the manufacturers to detect whether the e-coupons presented for clearing by the retailers have been redeemed after the purchase of goods at their stores.

5. THE BASIC MODEL PROTOCOL

Our scenario contemplates ℓ manufacturers, say $M_1, \ldots, M_\ell$, m advertisers, say $A_1, \ldots, A_m$, and n customers, say $C_1, \ldots, C_n$. For $i = 1, \ldots, \ell$, manufacturer M_i stipulates a contract with some of the advertisers and authorize them to release e-coupons on her behalf. Users visiting the advertisers' sites can download the e-coupons to purchase goods at M_i's web site.

E-coupon data authentication is provided by *message authentication codes (MACs)*, whose definition is given below [12]:

Definition 1. A message authentication code (MAC) algorithm is a family of functions h_k parameterized by a secret key k, verifying the following properties:

1. *ease of computation*: for a known function h_k, given a value k and an input x, $h_k(x)$ is easy to compute.
2. *compression*: h_k maps an input x of arbitrary finite bit-length to an output $h_k(x)$ of finite bit-length n. Furthermore, given a description of the function family h, for every fixed allowable value of k (unknown to an adversary), the following property holds:
3. *computational resistance*: given zero or more text-MAC pairs $(x_i, h_k(x_i))$, it is computationally infeasible to compute any text-MAC pair $(x, h_k(x))$ for any new input $x \neq x_i$ (including possibly for $h_k(x) = h_k(x_i)$ for some i).

As an example, our protocol could be implemented by using the MD5-MAC or the MAC algorithm based on DES block cipher. We refer the reader to [12] for an extended treatise on MACs.

We assume that for $i = 1, \ldots, \ell$, manufacturer M_i has been assigned a secret key k_{M_i} which is known only to her, and that for $i = 1, \ldots, \ell$ and $j = 1, \ldots, m$, there is a key k_{M_i,A_j} which is shared by M_i and A_j and is known only to them. For $i = 1, \ldots, \ell$ and $j = 1, \ldots, m$, let $h_{k_{M_i}}$ and $h_{k_{M_i,A_j}}$ be two MAC algorithm functions parameterized by k_{M_i} and k_{M_i,A_j}, respectively.

Initialization Phase. Manufacturer M_i provides the advertisers with a "framework" for the e-coupons to be released for a given period of time.

Let M_i be a manufacturer who is willing to advertise her products on A_j's web site. Merchant M_i releases to A_j an e-coupon framework which will be used by the advertiser to generate the e-coupons. This framework will be the same for both the static and the dynamic models. The framework released by the manufacturer carries

a) m_data: e-coupon specification data, such as,
   - M_name: the identity of the manufacturer;
   - P_name: the name of the promoted good;
   - O_name: type, value, and period of validity of the offer (discount on purchased items, three items for the price of two, gifts, samples, etc.);
   - A_name: the name of the advertiser.

b) $h_{k_{M_i}}(m\_data)$.

When an e-coupon is requested, the advertiser A_j generates an e-coupon according to the e-coupon framework received from the manufacturer. In addition to the above data, the e-coupon released by the advertiser A_j contains further information whose nature depends on the type of e-coupon we are considering.

First we will describe the information added by the advertiser to static e-coupons and then we will extend the protocol for the static model in order to make it work under the dynamic model.

5.1 Static E-coupons

In the static setting the e-coupon contains information which would allow the manufacturer to verify its validity.

Static E-coupon Generation. In the static setting advertiser A_j adds the following data to those specified in the e-coupon framework.

c) the serial number SN of the e-coupon;

d) $h_{k_{M_i,A_j}}(m\_data||SN)$.

The serial number increases every time a new customer downloads an e-coupon from the site. The serial number SN along with the m_data specified by the manufacturer constitute the e-coupon's significant data. The values $h_{k_{M_i}}(m\_data)$ and $h_{k_{M_i,A_j}}(m\_data||SN)$ are used for security reasons.

Static E-coupon Redemption. When manufacturer M_i is presented an e-coupon, then she computes the values $h_{k_{M_i}}(m\_data)$ and $h_{k_{M_i,A_j}}(m\_data||SN)$ and accepts the e-coupon if and only if these values coincide with those stored in the e-coupon and she has not seen an e-coupon with the same serial number SN.

5.2 Dynamic E-coupons

In the dynamic setting the e-coupon contains information which would allow the manufacturer to verify its release time.

In addition to $h_{k_{M_i}}$ and $h_{k_{M_i,A_j}}$, the protocol for dynamic e-coupons uses another publicly known function q which is assumed to be a *collision resistant* hash function according to the following definition.

Definition 2. A hash function $q : D \to C$ is collision resistant if and only if it is computationally infeasible to find a pair of distinct elements x and y of D such that $q(x) = q(y)$

Two examples of popular hash functions used in many practical applications are SHA-1 and MD5 (see [12]).

Dynamic E-coupons Generation. In the following we will suppose that the e-coupons' serial numbers are consecutive integers. In the dynamic setting, advertiser A_j will introduce the following information into the e-coupon:

c) SN: the serial number of the e-coupon;

d) $time$: the release time, i.e., the date and time at which the e-coupon has been downloaded;

e) u_data: a piece of information released by the customer (e.g., the customer's IP address number);

f) $q_{SN} = q(u\_data||q_{SN-1})$;

g) $h_{k_{M_i,A_j}}(m\_data||SN||time||u\_data||q_{SN})$.

Dynamic E-coupon Redemption. Our protocol assumes that a manufacturer may ask each advertiser for the list of the u_data's associated with the e-coupons released in a given time interval. For example, we may assume that every day a manufacturer obtains from each advertiser the list for the e-coupons released on the previous day. We assume that the u_data's are ordered according to their release time.

Let $u\_data_1, u\_data_2, \ldots, u\_data_z$ be the list of the u_data's for the e-coupons released in a given time frame by advertiser A_j on M_i's behalf, and let us assume, for the sake of simplicity, that the corresponding serial number be the integers $1, 2, \ldots, n$. Let q_0 denote the value of q computed for the last e-coupon released in the previous time frame. We say that the values $q_0, q_1, \ldots, q_z$ form a *dependence chain*. A manufacturer verifies the consistency of the sequence $q_0, q_1, \ldots, q_z$ by computing the values $q(u\_data_1, q_0), q(u\_data_2, q_1), \ldots, q(u\_data_z, q_{z-1})$, and by checking, for any $i = 1, \ldots, z$, if $q(u\_data_i, q_{i-1}) = q_i$. If for some i it results $q(u\_data_i, q_{i-1}) \neq q_i$ then we say that q_i violates the dependence chain. We assume that in every time frame the manufacturer verifies the

consistency of the dependence chain for the e-coupons released in the previous time frame. If the manufacturer finds a value q_i which violates the dependence chain, then she realizes that A_j is dishonest and takes the appropriate countermeasures.

When M_i is presented an e-coupon, she computes $h_{k_{M_i}}(m\_data)$, $h_{k_{M_i,A_j}}(m\_data||SN||time||u\_data||q_{SN})$ and checks whether these values coincide with those stored in the e-coupon. If the given e-coupon has been downloaded in some previous time frame, then the manufacturer disposes of the dependence chain for the e-coupons downloaded in that time frame, and consequently she can check whether the value q_{SN} in the e-coupon is equal to the corresponding element in that dependence chain. If the performed tests give positive result then the manufacturer accepts the e-coupon. If the given e-coupon has been downloaded in the same time frame it has been presented for redemption, then M_i performs only the first two tests and accepts the e-coupon if it passes these two tests. At the end of the time frame, she can retrieve the dependence chain and verify that the e-coupon has not been postdated. In fact we assume that the manufacturer is mainly interested in protecting herself against dishonest advertisers rather than in avoiding redemption of a few postdated e-coupons. Indeed, it is very important for her to detect an advertiser's misconduct which in the long run could seriously damage her advertisement campaign.

5.3 Protocol Soundness and Security

It is easy to see that if the advertisers behave correctly in the sense that they release e-coupons according to the manufacturer specifications, and if nobody manipulates, duplicates or falsifies e-coupons, then the protocol works properly.

Protection from unauthorized issuance of e-coupons. If the fake e-coupon is identical to a legally released one, in the sense that the values of all significant data in the e-coupon are the same as those of a legally released e-coupon, then it is actually a duplicate of the legal e-coupon. We will discuss later the security of our protocol with respect to duplicates.

Let us consider the case of a fake e-coupon which appears as an e-coupon released by advertiser A_j on M_i's behalf but which does not contain the same significant data of an e-coupon which has been legally released by A_j. Suppose that a dishonest person has seen a legally released e-coupon and wants to generate an identically structured e-coupon. She will modify the values of the e-coupon's significant data in order to make the terms of the promotion more convenient for her. In such a case the security problem represented by a fake e-coupon is exactly the same problem we have when a dishonest person manipulates the significant data of an e-coupon generated by an authorized advertiser according to the manufacturer specifications. For that reason this case can be assimilated to the case when a legally released e-coupon has been manipulated by a dishonest person. This case is discussed below.

Protection from e-coupon manipulation. We will show that our protocol allows a manufacturer to detect whether the e-coupon's significant data have been altered.

Suppose that a dishonest person wants to manipulate the data contained in an e-coupon released by A_j on M_i's behalf. If the dishonest person wants to modify the data specified by M_i then she replaces the original value of m_data in field a) with a different value m_data^*. In this case she should also replace the value $h_{k_{M_i}}(m\_data)$ with the value $h_{k_{M_i}}(m\_data^*)$ in field b) of the manipulated e-coupon. Recall that the no person other than M_i knows the key k_{M_i}. Consequently, the manipulator cannot directly compute $h_{k_{M_i}}(m\_data^*)$. Since the function $h_{k_{M_i}}$ is computation resistant, then it is computationally infeasible for the manipulator to compute $h_{k_{M_i}}(m\_data^*)$ for any value m_data^* different from the original value m_data. Consequently, the dishonest advertiser will introduce in field b) of the e-coupon a value different from $h_{k_{M_i}}(m\_data^*)$. On e-coupon verification, the manufacturer will compute $h_{k_{M_i}}(m\_data^*)$ and find out that this value is different from the one stored in the e-coupon. Consequently, she will reject the e-coupon.

Similarly the manipulator may alter the e-coupon's data specified by the advertiser. Let us denote with m_data^* and SN^* the values of m_data and SN in the manipulated e-coupon. If the e-coupon is dynamic, let $time^*$, u_data^* and q^* denote the value of $time$, u_data and q in the manipulated e-coupon.

In the static setting the manipulator should be able to compute the value $h_{k_{M_i,A_j}}(m\_data^*||SN^*)$, while in the dynamic case she has to compute $h_{k_{M_i,A_j}}(m\_data^*||SN^*||time^*||u\_data^*||q^*)$. Since she does not know k_{M_i,A_j}, then she cannot directly perform these computations. Moreover, since the function $h_{k_{M_i,A_j}}$ is computation resistant, then it is computationally infeasible for her to compute $h_{k_{M_i,A_j}}(m\_data^*||SN^*)$ or $h_{k_{M_i,A_j}}(m\_data^*||SN^*||time^*||u\_data^*||q^*)$. Consequently, the value of the function $h_{k_{M_i,A_j}}$ inserted in the e-coupon will be different from that of $h_{k_{M_i,A_j}}(m\_data^*||SN^*)$ in the static case, and from that of $h_{k_{M_i,A_j}}(m\_data^*||SN^*||time||u\_data^*||q^*)$ in the dynamic case. The manufacturer will discover this anomaly on e-coupon verification and will reject the e-coupon.

Protection from e-coupon double spending. Protection from e-coupon double spending is provided by means of the serial numbers. A manufacturer will accept a given e-coupon only from the customer which provides it for the first time. In this way a dishonest customer cannot benefit more than once of the same e-coupon. Further, she is

discouraged from giving out a duplicate of her e-coupon to another customer who might use it as first.

The manufacturer can avoid redeeming the same e-coupon more than once by simply maintaining a record of the coupons which have been already redeemed. Every time an e-coupon is presented to the manufacturer, its serial number is compared with those of the already redeemed e-coupons.

Protection from Postdated E-coupons. Notice that the serial number can be of help in preventing postdating attempts. Indeed, the serial number of an e-coupon carrying a certain emission date should be smaller than one carrying a later emission date. The advertiser does not know in advance how many customers will visit the site at the time she generates the postdated coupon, and, for that reason, she should generate an illegal coupon with a very faraway date to be sure she has enough serial numbers for the customers who will visit the site. However, the serial number does not guarantee that a postdated e-coupon will be detected. The only way to prevent the advertiser to postdate a given e-coupon is to introduce in each e-coupon pieces of information depending on previously released e-coupons. These pieces of information should be generable only with the cooperation of the customers who download the e-coupons. We have denoted such pieces of information with the term of u_data's. Indeed, suppose that C_c connects to the advertiser's web site before C_d and that the advertiser wants the e-coupon held by customer C_c to appear as to be downloaded after that of customer C_d. In this case the e-coupon of C_c should contain a piece of information dependent also on the information released later by C_d. Consequently, the advertiser in order to postdate the e-coupon of C_c must introduce a piece of information which violates the dependence relation from previously downloaded e-coupons.

Let $u\_data_1, u\_data_2, \ldots, u\_data_z$ be the list of the u_data's for the e-coupon released in a given time frame, and let us assume, for the sake of simplicity, that the corresponding serial number be the integers $1, 2, \ldots, z$. Let q_0 denote the value of q computed for the last e-coupon released in the previous time frame. Suppose that an advertiser and a customer have colluded in order to postdate an e-coupon in the above list. Assume that the postdated e-coupon has been downloaded at time t_1 soon after the one carrying serial number r. Suppose that instead of carrying the serial number $r+1$ and $time = t_1$, the postdated e-coupon carries serial number $SN = s$ with $s > r+1$, and $time = t_2$, with $t_2 > t_1$. If a honest customer visits the site at time t with $t_1 < t < t_2$, then the advertiser releases to him an e-coupon with $time = t$ and a serial number v comprised between r and s. Obviously the value q_s in the illegal e-coupon should depend on the u_data value of the e-coupon downloaded at time t. Since these data are not available at time t_1, then the value q_s computed by the advertiser violates the dependence chain. The manufacturer can detect this anomaly when she checks the consistency of the sequence $q_0, q_1, \ldots, q_z$. To avoid this situation the advertiser should postdate all the e-coupons downloaded between time t_1 and time t_2. Hence, the u_data's of all these e-coupons will appear in the manufacturer's list after the u_data of the illegal e-coupon. In other words the advertiser should convince the manufacturer that these e-coupons have been downloaded after time t_2. Since the customer who downloads the e-coupon at time t is honest, then she should not realize that her e-coupon has been postdated. Consequently, her e-coupon should carry the exact release time, that is $time = t$. Obviously the dishonest customer who has downloaded the postdated e-coupon will certainly redeem it. Suppose that also the customer who has downloaded the e-coupon at time t decides to redeem her e-coupon. Then, the manufacturer will find out that the $time$ value of this e-coupon is anterior to that of the postdated e-coupon. Since this order does not correspond to the order of the u_data's of the two e-coupons in the list, then the manufacturer will detect the illegal misconduct of the advertiser who released those e-coupons.

The above verification procedure succeeds to detect a postdating attempt if and only if a honest user redeems an e-coupon which has been downloaded in the time interval elapsing between the time t_1 the dishonest user has actually downloaded the e-coupon and the time t_2 carried by the postdated e-coupon. Obviously, one cannot hypothesize that such a circumstance should necessarily occur. The manufacturer can force such a circumstance by downloading herself e-coupons from the advertisers' sites. In this way the manufacturer simulates the behavior of a honest user and obtains e-coupons which carries the exact release time. To make this stratagem effective, the manufacturer will visit the advertisers' web sites at random times so that the advertisers cannot make assumptions on when the manufacturer will download an e-coupon and is forced to behave honestly.

6. EXTENDED MODEL PROTOCOL

In this model, the scenario comprises ℓ manufacturers, say $M_1, \ldots, M_\ell$, m advertisers, say $A_1, \ldots, A_m$, n customers, say $C_1, \ldots, C_n$, and p retailers, say $R_1, \ldots R_p$. Manufacturer M_i, $i = 1, \ldots, \ell$, may authorize some of advertisers $A_1, \ldots, A_m$ to release e-coupons on her behalf. Users visiting the advertisers' sites can download the e-coupons to purchase goods at any of retailers $R_1, \ldots R_p$ selling M_i's products.

As in the protocol for the basic model, we assume that for $i = 1, \ldots, \ell$, manufacturer M_i has been assigned a secret key k_{M_i} and that for $i = 1, \ldots, \ell$ and $j = 1, \ldots, m$, there is a key k_{M_i,A_j} which is known only to M_i and A_j. We also assume that for $i = 1, \ldots, \ell$ and for $h = 1, \ldots, p$, there is a key k_{M_i,R_h} which is known only to M_i and R_h.

For $i = 1, \ldots, \ell$ and $j = 1, \ldots, m$, we denote with $h_{k_{M_i}}$,

$h_{k_{M_i,A_j}}$ and $h_{k_{M_i,R_h}}$ three MAC algorithm functions parameterized by k_{M_i}, k_{M_i,A_j} and k_{M_i,R_h}, respectively.

The initialization phase as well as the e-coupon generation phase are the same as those in the protocol for the basic model. As in the basic model, we have a protocol for static e-coupons and a protocol for dynamic e-coupons.

E-coupon verification. Let R_h be a retailer selling M_i's merchandise. Suppose that a customer presents an e-coupon to retailer R_h to obtain a discount on the purchase of some merchandise produced by manufacturer M_i. In e-commerce transactions, payments are usually made by credit card, money order, bank transfer, or other similar mechanisms. Hence, we can assume that the transaction is settled only after the payment or a proof of the payment has been received by the retailer. Such payments have a code associated which identifies the institute authorizing the payment, the import paid, and the date of the purchase. We will refer to these identification codes with the term of *invoice number* and denote them by IN. When R_h sends the e-coupon to M_i for the verification, she also sends the invoice number of the corresponding transaction. M_i computes the values $h_{k_{M_i}}(m\_data)$, $h_{k_{M_i,A_j}}(m\_data||SN)$ and accepts the e-coupon if and only if these values coincide with those stored in the e-coupon and if she has not seen an e-coupon with the same serial number SN and the same invoice number IN.

6.1 Protocol Soundness and Security

The soundness and the security of the protocol as far as it concerns protecting the manufacturer from unauthorized issuance of e-coupons, e-coupon manipulation, e-coupon double spending, and in the dynamic setting, from postdated e-coupons, can be proved by using the same arguments used for the protocol for the basic model. It remains to prove that the protocol guarantees also protection from unredeemed e-coupons.

Protection from unredeemed e-coupons. The system allows the manufacturer to detect unredeemed e-coupons. Indeed, the manufacturer can keep track of the invoice numbers attached to the e-coupons which she has been asked to verify, as well as of the identity of the retailers who forwarded the e-coupons to her. A retailer who tries to be reimbursed for an unredeemed e-coupon should introduce into the e-coupon either a dummy invoice number or the invoice number of some past commercial transaction. The manufacturer can detect whether the invoice number corresponds to a commercial transaction which is bound to a previously redeemed e-coupon by checking the IN's list in her database. If she does not find the invoice number in her list, she can detect whether the invoice number is a dummy one by requesting a control to the institute which made the payment. The invoice number allows also the manifacturer to determine when the transaction has occurred and to control the correspondence of the date with the associated clearing request of the advertiser.

7. IMPLEMENTATION

Once the model of the e-coupon has been designed, it is necessary to design also the techniques for handling the e-coupons during all the interactions among the clients, the advertisers, and the manufacturers. Since one of the requirements of an e-coupon exchange infrastructure is to maintain a low complexity for all the participants to the protocol, we devise a lightweight implementation of our model. In particular we are developing a prototype which is based on CGI scripting to perform server side computation (on the advertiser and the manufacturer web sites), and a plugin to perform client side computation.

Our proposal has the advantage of reducing as far as possible the changes to the usual client-server communication pattern over Internet. An e-commerce site which would like to implement our technique for e-coupon distribution, should only provide the right scripts while the customers wanting to exchange e-coupons have to download and install the developed plugin. Alternative kinds of server side computation are being explored to improve performance, such as scripting languages (PHP or ASP) and modification to be done to the web server (developing a module to be used in conjunction with the Apache web server).

7.1 Size of an E-Coupon

Since the e-coupon is used during the interactions between the customer and the manufacturer, and the customer and the advertiser, it is important to limit the size of the e-coupon, to avoid a communication overhead for the user. In the following we analyze the size of an e-coupon constructed according to the requirements described in Section 5.

We will use a MAC algorithm based on a DES block cipher to implement the functions $h_{k_{M_i}}$ and $h_{k_{M_i,A_j}}$. Both keys k_{M_i} and k_{M_i,A_j} are 56-bit DES key. In the static case, each e-coupon will be composed of the m_data which can be of arbitrary length, and of a sequence of 160 bit containing: the results of the computation of the two hash functions $h_{k_{M_i}}$ and $h_{k_{M_i,A_j}}$, each one 64 bit long and the serial number SN (32 bit long). Assuming 100 bytes for each field constituting the m_data (i.e., M_name, A_name, P_name, O_name), the total length of a static e-coupon is approximately of 420 bytes.

A dynamic e-coupon will also have 6 bytes for the generation time and 4 bytes containing the user data (the user's IP address). A dynamic e-coupon will have then 30 bytes in addition to those of a static one, for a total length of approximately 450 bytes.

7.2 The Initialization Phase

During the initialitazion phase of the protocol the advertiser and the manufacturer agree on the terms of the

advertisement campaign. During this phase, the manufacturer has to communicate to the advertiser the e-coupon specification as described in Section 5. Such communication can be done off-line or using some secured channel. After this communication, the advertiser is able to set all the parameters for the e-coupon generation.

In the dynamic setting, eventually the advertiser and the manufacturer interact also during the advertisement campaign. Indeed, in order to increase the control on the advertiser's activity, the manufacturer can split the duration of the advertisement campaign in several time frames (e.g., one day), at the end of which the advertiser is obliged to provide the log file relative to the generated e-coupons. The manufacturer can use that information to reconstruct the generation process and to recognize any possible postdating attempt by the advertiser. The verification is performed off-line, by examining the log file relative to the elapsed time frame, and following the e-coupon dependence chain to control the correctness of its generation with respect to the received e-coupons.

7.3 The Generation Phase

The e-coupon generation phase is started when the customer actively chooses the discount offer or when she is visiting the page containing the e-coupon. This implies that in both cases some server side computation is started to produce a freshly generated e-coupon with the offer on a particular product.

Any application designed to handle e-coupons has to provide some means to store the e-coupons and the contained data. The place where e-coupons are stored and successively retrieved is commonly called user's "wallet". Each buyer can access her wallet to examine the e-coupons collected during her visits on the advertisers' sites and eventually use one of them in order to purchase of a product.

In our model, we assume that the interaction between clients and advertisers is started when a customer chooses to accept an attractive offer hosted in the advertiser's site. In this case the e-coupon is presented as a link (or a banner) containing a particular mime-type which activates the client plugin. The plugin can be downloaded from the manufacturer site, which can control in this way the right functionalities of the plugin code, avoiding collusion between the customer and the advertiser. After clicking on an e-coupon link (the customers have then an active role) the e-coupon plugin is executed with the task to control the validity of the e-coupon, to verify that the advertiser has correctly generated the e-coupon, and to store it in a file which is hosted on the client hard disk. On the other side, the advertiser's CGI script generates the e-coupon by collecting all the data relative to the e-coupon (the updated serial number, the m_data and the IP address contained in the client http request), calculates the hash values of both the data and the dependence chain, and stores the user data in a file which successively would be communicated to the manufacturer for the verification.

7.4 The Redemption Phase

When the customer decides to use one of the e-coupons contained in his wallet to purchase some merchandise, the redemption phase is started. The e-coupon has the address of the web site where the purchase can be made, and extra data. This phase involves the sending of data from the customer to the manufacturer, who must perform some extra computation to verify that the e-coupon is valid and that the purchase can be finalized.

On the client side, e-coupons are stored in a local file which is used by the browser to visualize all the e-coupons contained in the wallet. The file which is generated by the plugin contains html code for each e-coupon, which is then represented by the URL of the manufacturer plus extra data constituting the body of the e-coupon. Since no further computation is requested on the client side, it is not necessary to activate the plugin, but the data which are contained in the e-coupon are sent to the manufacturer through an HTTP GET request. Whenever the customer wants to redeem an e-coupon he clicks on the e-coupon establishing a connection between the browser and the manufacturer site. The CGI script running on the manufacturer site at the URL contained in the e-coupon has the task to accept the e-coupon, to verify its validity and eventually finalize the purchase applying the conditions of the offer. The verification in this phase aims to control the well-formedness of the e-coupon sent by the customer. An additional verification phase is conceived to control the advertiser's activity in the process of the e-coupon generation. This kind of verification can be performed off-line, and the validity of a received e-coupon can be controlled by simulating the generation of e-coupons, following the list of data provided by the manufacturer and controlling that all the received e-coupons have been correctly constructed.

7.5 Handling Electronic Purchase Proofs

The handling of the purchase proofs exploits the same mechanisms described above for the handling of e-coupons. Indeed, we are developing the functions for collecting and redeeming the proofs as extensions of the functionalities of the previously described plug-in. In the basic model, the plug-in stores the purchase proof attached to a product sold by the manufacturers in the customer's wallet. Whenever the customer decides to reuse the proof she must upload to the manufacturer the corresponding bit string contained in its wallet. During the verification phase, the manufacturer has to perform some simple hash operations to control the validity of the presented proof. In the extended model, the retailer must perform some additional operation to attach the transaction number to the proof provided by the manufacturer.

8. SOME CONCLUSIONS

In this paper, we provided a suitable model for e-coupons such that a number of security assumptions can

be done on their generation and distribution. We presented also two protocols which respect the security requirements and discussed several usage patterns involving both e-coupons and electronic purchase proofs. Our model is deliberately lightweight with respect to other proposals [10] which make use of digital signatures. We want to point out that our protocols involve no registration by customers who want to download e-coupons from advertisers' web sites. This is a big improvement with respect to the e-coupon distribution systems currently used by most advertisers' web sites. Indeed our protocols attains the security requirements while preserving customers' anonymity.

The prototype implementation described in Section 7 shows the evidence that our proposal reduces the overhead necessary to handle all the different phases of the protocol. On the other hand, our model shows the same security features which guarantee each participant against malicious behavior of any other participant to the protocol.

We are considering some improvements to our protocol, in order to make it work in a more general context. In particular we are concerned with the problem of verifying the e-coupon generation time. Indeed, in the dynamic setting, our protocol relies on the fact that at least one honest user redeems a legally released e-coupon. However, we may assume that a manufacturer might play the role of a honest user who downloads e-coupons from the advertisers' sites at random times. In order to relax such assumption, we are considering the application of timestamping techniques [8] to improve the mechanism of e-coupon generation, so that both customers and manufacturers increase their confidence in the advertisers' activity.

9. REFERENCES

[1] R. Anand, M. Kumar, and A. Jhingran. Distributing e-coupons on the Internet. In *9th Conference on Internet Society (INET '99)*, San Jose, 1999.

[2] R. Anand, M. Kumar, A. Jhingran, and R. Mohan. Sales promotions on the Internet. In *Third Usenix Workshop on E-Commerce*, Boston, 1998.

[3] J. Black, S. Halevi, H. Krawczyk, T. Krovetz, and P. Rogaways. UMAC: Fast and Secure Message Authentication. In *Advances in Cryptology - CRYPTO '99. Lecture Notes in Computer Science*, pages 216–233, vol. 1666, Springer-Verlag, 1999.

[4] C. Blundo, A. De Bonis, and B. Masucci. Metering schemes with pricing. In M. Herlihy, editor, *14th International Conference on Distributed Computing (DISC 2000)*, volume 1914 of *Lecture Notes in Computer Science*, 2000. Springer-Verlag, Berlin.

[5] S. Cimato and A. De Bonis. Online advertising: secure e-coupons. In A. Restivo, S. Ronchi Della Rocca, L. Roversi editor, *7th Italian Conference on Theoretical Computer Science (ICTCS 2001)*, volume 2202 of *Lecture Notes in Computer Science*, Torino, Italy 2001. Springer-Verlag, Berlin.

[6] M. Franklin and D. Malkhi. Auditable metering with lightweight security. In R. Hirschfeld, editor, *Financial Cryptography (FC '97)*, volume 1318 of *Lecture Notes in Computer Science*, pages 151–160. Springer-Verlag, Berlin, 1997.

[7] R. Garg, P. Mittal, V. Agarwal, N. Modani. An Architecture for Secure Generation and Verification of Electronic Coupons. In *Proceedings of 2001 USENIX Annual Technical Conference*, Boston, Massachusetts, USA.

[8] S. Haber and W.S. Stornetta. How to time-stamp a digital document. *Journal of Cryptology*, 3(2):99–111, 1991.

[9] IBM India Research Lab. E-coupons. `http://www.research.ibm.com/irl/projects/ecoupons/`.

[10] M. Jakobsson, P. D. MacKenzie, and J. P. Stern. Secure and lightweight advertising on the web. In *9th World Wide Web Conference (WWW9)*, 1999.

[11] Joint Industry Coupon Committee. Coupons: a complete guide. Grocery Manufacturers of America, 1998.

[12] A. Menezes, P. van Oorschot, and S. Vanstone. *Handbook of Applied Cryptography*. CRC Press, 1996.

[13] M. Naor and B. Pinkas. Secure and efficient metering. In K. Nyberg, editor, *Advances in Cryptology – Eurocrypt '98*, volume 1403 of *Lecture Notes in Computer Science*, pages 576–590, Espoo, Finland, 1998. Springer-Verlag, Berlin.

[14] New York Times (C. Greenman). The trouble with rebates, September 16, 1999.

[15] New York Times (M. Slatalla). Turning coupon users from clippers into clickers, April 1, 1999.

[16] New York Times (B. Tedeschi). Is coupon clicking the next advertising trend?, May 12, 1998.