A Security Analysis of the Danish Deposit Return System

Ivan Garbacz, Rosario Giustolisi, Kasper Møller Nielsen, Carsten Schuermann

IT University of Copenhagen, Denmark
{ivga,rosg,kmni,carsten}@itu.dk

Abstract. The process that allows one to get rewarded for returning a container through reverse vending machines (RVM) involves people and technology. In fact, it typically sees a set of human parties (e.g. customers, cashiers) and technical parties (e.g, RVMs, databases, scanners) to collaborate in order to enable effective recycling. In this paper, we advance a formal treatment of the Danish Deposit Return System (DRS). We investigate the security of the ceremony that people are expected to perform in the context of DRS using field observation and automated reasoning tools. We give a particular focus to the security threats due to people interacting with the technology behind DRS. The findings of our investigation enable novel considerations of the ceremony weaknesses and make it possible to delineate potential mitigations.

1 Introduction

The introduction of technology into everyday life is normally considered secure, as are the companies providing such technology. Examples include automatic bike rental systems, online food ordering services, or, as we discuss in this paper, automatic deposit-return systems for cans and bottles, as they are commonly used all over Denmark. However, it is difficult to state precisely what security of such systems means and what it would imply. The reason is that socio-technical systems have a completely different attack surface than purely social systems, where interactions are human to human, or purely technical systems, where the operational context is deemed irrelevant. This attack surface can be, if not properly considered, a threat to confidentiality of private information, or in our case, the financial soundness of transactions, and therefore to the reputation of the company deploying the technology or its suppliers.

In this paper, we consider a *ceremony* as a technical system extended with its human users [3] and demonstrate that an analysis of the processes defining the ceremony can yield insights that protect the company's assets, its brand and its reputation. We study the different Danish bottle and can deposit return system (DRS) deployed in Danish supermarket chains Kvickly, Coop, and Netto, and analyse formally the security ceremonies that they require using automated reasoning tools. All DRS under consideration use a paper-based voucher system, generated by a reverse vending machine (RVM) and refunded by the cashier. In our study, we focus on three simple security requirements (1) if a voucher was

cashed, then bottles of corresponding deposit value were indeed returned, (2) if a voucher is redeemed for a value, then the voucher was printed on an eligible RVM machine, and (3) a voucher cannot be used more than once.

The main contribution of this paper is that it is possible to reason about security ceremonies of this kind, with field observation and formal tools, and that interesting observations can be made about the security of Danish DRS.

The mechanised argument is carried out in Tamarin [10]. In order to define an appropriate model, we reverse engineer the DRS technologies in use and the accompanying processes, as we had no access to design documents, implementation or process definition details. From the knowledge gathered this way, we devise different socio-technical security contexts, which we model through different behavioural actions of inattentive customers or neglectful employees. In summary, the formal analysis approach makes the notion of DRS security more precise: some DRS are reasonable secure with respect to our model, while others are completely insecure. Some DRS could even be tricked into accepting counterfeit vouchers of arbitrary value that could easily be generated on a thermal printer at home.

Outline. This paper is organised as follows. In Section 2 we describe our reverse engineering activities resulting in a model of the security ceremony for different Danish DRS. In Section 3 we detail the formal analysis including the different behavioural actions. Our model includes some technical but mostly rules modelling humans. In Section 4, we assess results and describe our findings. In Section 5, we discuss related work before we conclude in Section 6.

2 Modelling the Ceremony

In Denmark, the deposit return scheme is typically implemented by supermarket chains through reverse vending machines (RVM). The customer experience is similar, independent of the store. However, different supermarket chains use different technology, and hence the technical protocol may vary although this is transparent to the customer. For example, RVMs deployed in Kvickly and Coop supermarkets are similar, but they produce different vouchers compared to the RVMs deployed in Netto supermarkets.

Since there is hardly any information about the technology behind deposit return systems available, besides a few patents, this work follows a reverse engineering approach and reconstructs the technical aspects and the ceremony of DRS. In particular, this work adopts the road map for reverse engineering proposed by Müller et al. [11] and focuses on field observation as a primarily investigative technique to gather information regarding the ceremony.

2.1 The Reverse Vending Machines

Reverse vending machines (RVM) are the main technological element in the DRS, hence it is essential to gather as much information as possible regarding

the functioning of RVMs to build a correct ceremony. Most of the RVMs in Denmark are built by Tomra, and their specifications available to the public in the form of patents. This work considers three Tomra machine models: T-710, T-820, and T9. Every machine is built into a wall, which has a room on the other side which can be accessed through a locked door. An RVM can either accept a single empty container at a time or a beverage crate. Each container is validated on the basis of its weight, barcode, and size. In general, an RVM accepts only glass containers that have a barcode. The sole exemption is the traditional shape of the Danish beer bottle, which does not need to be equipped with a barcode for being accepted. Cans, instead, are accepted with or without barcode. However, the latter case entails no reward for the customer.

From a security perspective, Tomra has filed several patents for detecting fraud attempts in reverse vending machines [12,17,7]. However, the effort is almost exclusively concentrated on making sure that the machine does not accept invalid containers. Thus, we can assume that no RVM would accept an invalid container. Such an assumption can be confirmed by our observations of the machines. In particular, we had access to look through one of the Tomra RVMs while being emptied from its containers.

Fig. 1: An example of a voucher printed by a Tomra T-710 machine

In Denmark, RVMs are equipped with thermal printers that print paper vouchers. A voucher attests the number of containers filled by the customer and entails a reward to them. An example of a voucher is in Figure 1. A voucher includes the following information

– The redemption value in Danish kroner

– A machine-readable serial number (SN1)
– The number of containers
– The model of the RVM
– A non-machine-readable serial number (SN2)
– Time and date of the printing of the voucher

2.2 The Machine-Readable Serial Number (SN1)

To the best of our knowledge, there is no document covering how the RVM generates the information included in the voucher, especially how the serial numbers are generated. According to the patents filed by Tomra [6,16], the company has implemented some security measures against presentation of home-made vouchers. In particular, some RVMs implement voucher control by means of a communication from the RVM to a cloud-based service solution provided by Tomra [20]. Once the filling of the RVM is completed by the customer, the RVM generates the voucher and sends both redemption value and SN1 to the Tomra servers. When later the voucher is presented for rewarding, this is controlled against the Tomra server, which authorises the payment to the customer. According to the patents, other solutions that do not require constant communication with the Tomra server may be implemented. For instance, the RVM can be set to communicate locally with a computer hosted at store premises, which periodically updates the list of valid vouchers to the in point of sale stations.

Since no public specification of SN1 is available, we have derived it empirically by analysing the vouchers printed by the different Tomra machines this work has taken in consideration (i.e. T-710, T-820, T9) hosted in three different stores (i.e. Kvickly, Coop, and Netto). Kvickly and Coop belong to the same supermarket chain. In our case, the Kvickly store hosts three T-710 machines, the Coop store hosts two T-820 machines, and the Netto store hosts one T9 machine.

Kvickly and Coop Stores. Several vouchers with different values were collected at different times and dates. A sample of the batch of vouchers collected at Kvickly from a T-710 is in Figure 2a. It can be seen that, independently from date and time, SN1 is fixed when the RVM is filled with one container worth of 1.00 Kr. However, SN2 still slightly changes. This is because the three vouchers in Figure 2a were printed by three different machines. This is confirmed by the second batch of vouchers (see Figure 2b) obtained from the same store. The second batch also reveals that SN1 slightly changes accordingly the value of the containers filled in the RVM. The first nine digits are always fixed while the 10^{th} and the 13^{th} digits change. It can be seen that the 10^{th} digit represents the total value of the voucher. It is also confirmed that the same approach is used at the Coop supermarket as depicted in Figure 2c. Here the 2^{nd} digit of the SN1 digits changes because the voucher is printed in a different store. However, the rest of the SN1 reflects the value of the containers.

Finally, in order to fully predict all the digits of the SN1, it is necessary to understand how the last digit is generated. We found that the last digit $SN1_{13}$ is the check digit from the EAN-13 standard, which can be computed as

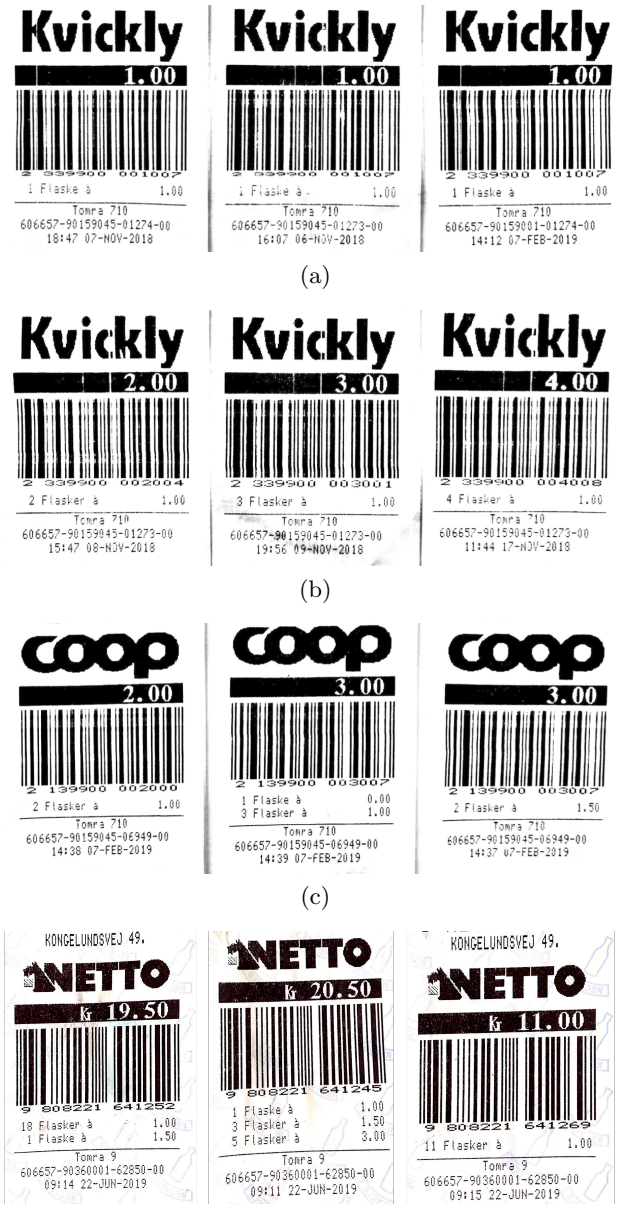

Fig. 2: The four different batches of vouchers obtained from different Tomra machines at Kvickly, Coop, and Netto. (a) the SN1 digits are fixed in each voucher; (b) some of the SN1 digits reflect the value of the voucher; (c) only the 2^{nd} digit differs among Kvickly and Coop stores; (d) the SN1 digits increment by one unit at Netto

$\text{SN1}_{13} = x - y$ where

$$y = \text{SN1}_{[1\ldots12]} \cdot [1\ 3\ 1\ 3\ 1\ 3\ 1\ 3\ 1\ 3\ 1\ 3] \ \wedge \ x = \lceil y \rceil \text{ s.t. } x \ mod\ 10 = 0$$

For example, the SN1 in Figure 1 can be computed as

$$\begin{aligned} y &= [2\ 3\ 3\ 9\ 9\ 0\ 0\ 0\ 0\ 4\ 0\ 0] \cdot [1\ 3\ 1\ 3\ 1\ 3\ 1\ 3\ 1\ 3\ 1\ 3] \\ &= 2 + 9 + 3 + 27 + 9 + 0 + 0 + 0 + 0 + 12 + 0 + 0 = 62. \\ x &= \lceil 62 \rceil = 70 \end{aligned}$$

$\text{SN1}_{13} = x - y = 70 - 62 = 8.$

Netto Stores. The T9 machine at Netto generates the SN1 in a different way. It can be seen that the value of the voucher is not anymore reflected on any of the SN1 digits. Instead, by analysing three vouchers printed in sequence by the machine, we found that the SN1 is implemented as a counter that increments by one unit every time a voucher is printed. Notably, the SN1 digits can be also fully predicted at Netto stores since the last digit of the SN1 is still a check digit from the EAN-13 standard.

Discussion. The analysis of the vouchers printed at Coop confirms that the SN1 and all the other information printed in the vouchers can be fully predicted. Since a voucher can be redeemed at any of the stores of the same supermarket chain, we can rule out that barcodes are sent to the store's local computer. Also, since any two vouchers with the same value turn out to contain the same SN1, it is unclear how the Tomra servers can prevent a fake voucher to be redeemed provided that other vouchers with the same value where printed. We believe that in this case there is no communication from the RVM and that the scanner reads the value of the voucher from the SN1 only. However, as we shall see later, we assume that such communication exists in the formal analysis of the Kvickly and Coop DRS ceremony.

Netto stores have a different way to generate the SN1, and the value is not stored in the SN1. Thus, we believe that the RVM should communicate to either Tomra servers or a store's local computer the details of the voucher. However, as for Kvickly and Coop stores, the SN1 is still fully predictable, but in this case one needs to know the value of the counter of the RVM.

2.3 Ceremony Description

Having seen the modelling of RVM and SN1, we can present a full description of the ceremony, as depicted in Figure 3. It begins with the customer approaching the RVM and inserting a number of containers (step 1). The RVM may either accept or reject each of the containers. It will stop accepting new containers when either the customer pushes the button to complete the filling phase or the

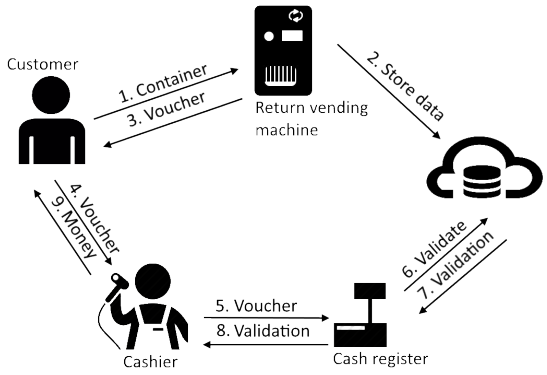

Fig. 3: The Danish deposit return system ceremony

RVM is full and cannot accept further items. Then, the RVM generates the data to be printed in the voucher, and, optionally sends them to the Tomra servers (step 2). The RVM prints the voucher (step 3) that can be redeemed at the cash register at *any* of the stores belonging to the supermarket chain (step 4). There, the cashier scans the barcode encoding the SN1 (step 5). As seen above, the cash register may check the validity of the voucher against the Tomra server or a local computer (step 6 and 7). Then, the cashier may either stamp the voucher with the supermarket mark or rip it and put it in the cash register (step 7). Finally, the cashier reads the import redeemable from the cash register (step 8) and hands to the customer the money matching the value read from the cash register (step 9).

3 Formal Analysis

We analyse the ceremony of the Danish DRS using an automated tool for the formal verification of security protocols. Besides the modelling of the technological part of the DRS ceremony, it is required to model behaviours of the people interacting with the DRS. Thus, we model *behavioural actions* that people may perform as an extension of the canonical description of the ceremony. A behavioural action may or may not be prescribed by the ceremony. In the latter case, they may produce a deviation from the canonical description of the ceremony. For example, the action in which a cashier throws away a voucher is a consistent action with respect to the DRS ceremony and represents a possible deviation from its canonical description. The goal of the analysis is to check whether such deviations affect the security of the ceremony. Thus, three behavioural actions are derived as follows

– *the aware humans*, in which no one deviates from the canonical description of the ceremony;

– *the inattentive customer*, in which customers may share their vouchers with other parties (possibly the attacker);
– *the unaware cashier*, in which the cashier may throw a voucher somewhere else than the cash register.

The three behavioural actions outlined above are not meant to be comprehensive but includes what we think are the most basic ones for the DRS case. They mainly serve to demonstrate the viability of analysis security ceremony using a formal approach. Also, they enable one to assess whether the ceremony is secure despite the deviations that originate from the actions.

The Tamarin Prover. Tamarin [10] is an interactive protocol verifier that can prove reachability and equivalence-based properties in the symbolic model. It has an expressive language based on multiset rewriting rules and comes with a built-in attacker model (i.e. the Dolev-Yao attacker). However, it allows one to specify any threat model. Each rule operates on a multiset of facts and has a premise and a conclusion. Facts are predicates that store state information and may be linear (i.e. can be consumed only once) or persistent (i.e. can be consumed arbitrarily often by rules). The execution of the rules creates a labelled transition system of the protocol in which all facts in the premise of a rule are consumed by the facts in the conclusion.

3.1 Modelling Choices

Modelling a security ceremony into a symbolic model requires one to make some abstraction choices. The first choice is to develop the equational theory needed to model the ceremony. The equational theory allows one to model arbitrary cryptographic and non-cryptographic functions. In the case of the DRS ceremony, we model the following non-trivial functions

Table 1: Part of the equational theory to model the DRS ceremony in Tamarin

$(*Voucher\ scanning*)$	$getVoucherLeft(voucher(SN1, value)) = SN1$
$(*Voucher\ scanning*)$	$getVoucherRight(voucher(SN1, value)) = value$
$(*Cash\ out*)$	$getMoney(money(value) = value$

The function *voucher* captures the printing of a voucher by the RVM. The function *getVoucherLeft* captures the scanning of the voucher and returns the SN1. Similarly, the function *getVoucherRight* gets in the voucher and returns the value of the voucher. Finally, the function *getMoney* models the cashier handing to the customer the amount of money matching the value read from the cash register.

Another modelling choice regards the modelling of physical objects such as vouchers or money. The presence and the handing over of physical objects are typical of ceremonies since they involve people. However, physical objects are normally not modelled in security protocols as these involve only the exchange of pieces of information. The main difference between objects and pieces of information is that the former cannot be reproduced and once they are handed over, they are not anymore available to the sender. Conversely, a piece of information can be replicated, stored, and made available to the sender. In Tamarin, handing and getting an object can be elegantly modelled using linear facts, in which resources are expandable. The sending and the receiving of pieces of information are modelled using persistent facts.

Another important choice regards the modelling of SN1 barcodes. We have seen that in Kvickly and Coop stores the SN1 is a function of the number of containers filled into the RVM. Hence, we model the SN1 barcode accordingly. For simplicity, we assume the number of containers to be constant. This is not the case for Netto stores, in which the SN1 barcode is a function of the previous barcode. Here, we model the SN1 as a random value, otherwise the verification in Tamarin may incur into non-termination. Note that this is a securely sound over-approximation of the model since, as we have seen before, the SN1 is predictable provided one knows the previous barcode printed by the RVM. However, we assume that the attacker has no access to such barcode (but he may have access to other barcodes). This assumption is sound since any attack found in such a scenario would be valid also in the scenario where the barcode can be predicted.

3.2 Human Rules

Behavioural actions can be easily modelled in Tamarin as rules. For reason of space, we comment only on the main rules of the ceremony that model behavioural actions[1]. The rule that expresses a customer receiving a voucher from the RVM (i.e. step 3 of the ceremony) and handing it to the cashier (i.e. step 4 of the ceremony) can be modelled as

```
rule H1SendToH2:
     [AgSt($H1,'H1_1',conts_I),In_O($V,$H1,'voucher_VToH1',voucher_O)]
     --[H1SendToH2($H1,voucher_O,conts_I)]->
     [AgSt($H1,'H1_2',conts_I),Out_O($H1,$H2,'voucher_H1ToH2',voucher_O)]
```

This rule is part of the canonical description of the ceremony, hence it contributes to the modelling of the aware humans. In the premise, the fact `AgSt` expresses a customer `H1` who knows how many containers have been filled `conts_I` and receives the `voucher_O`. In the conclusion, the customer hands the voucher to the cashier `H2` but memorises how many containers have been filled out. The suffixes $\_I$ and $\_O$ stand for information and object respectively. Information

[1] The full Tamarin code is available at the link `https://www.dropbox.com/s/qrinq3yc9kkrq4e/DRS_Tamarin.zip?dl=0`

facts are kept on conclusions while object facts are not. Handing is captured by channels `In_O` and `Out_O`, which are modelled as linear facts.

The rules concerning the inattentive customer can be summarised as

```
rule H1SendToBadH:
     [AgSt($H1, 'H1_1', conts_I), In_O($V, $H1, 'voucher_H1ToH2',voucher_O)]
     --[H1SendToBadH($H1, voucher_O, conts_I)]->
     [AgSt($Badh, 'H1_2', conts_I),
      Out(<getVoucherLeft(voucher_O),getVoucherRight(voucher_O),$H1>)]

rule H2GetFromBadH:
     [AgSt($H2,'H2_0', validation_I), In(<voucher_O, $Badh>)]
     --[H2GetFromH1($H2, voucher_O, validation_I)]->
     [AgSt($H2, 'H2_1', <voucher_O, validation_I>),
      Out_O($H2, $Re, 'voucher_H2ToRe',voucher_O)]
```

The rule `H1SentToBadH` is similar to the canonical rule seen above for the aware humans, but with a different conclusion, in which the customer hands the voucher to the attacker. In this case, only `H1` appears in the fact `Out` since the recipient is the attacker. Similarly, the rule `H2GetFromBadH` enables the cashier to get a voucher from any one, including the attacker. These rules deviate thus extend the canonical description of the DRS ceremony.

The unaware cashier can be captured with a rule that specifies another deviation from the canonical description of the ceremony. In Tamarin, this is modelled as

```
rule H2SendToH1andThrowsIt:
     [AgSt($H2,'H2_1', <voucher_O, validation_I>)
      ,In_I($Re,$H2,<'value','verification'>,<value_I, verification_I>)
      ,In_O($Re, $H2, 'money_ReToH2', money_O)]
     --[H2SendToH1($H2, voucher_O, validation_I, verification_I,
        money_O, value_I),
        Eq(validation_I, verification_I)]->
     [Out_O($H2, $H1, 'money_H2ToH1', money_O),
      Out(<voucher_O, verification_I>)]
```

In the premise of the rule, the cashier `H2` receives a signal from the cash register `Re` about the validity `verification_I` of the voucher (step 6). In the conclusion, the cashier hands the money to the customer (step 9) and throws away the voucher, which becomes available to the attacker.

4 Findings

We analyse the DRS ceremony against three security requirements

- *Cash for container*, which says that if a voucher is redeemed for a value, then some containers of equal value should have been returned earlier.
- *Cash for voucher*, which says that if a voucher is redeemed for a value, then a voucher was actually printed by an RVM.

– *Unique voucher*, which says that a voucher can be used only once to get money.

The three requirements above capture what we believe are the basic security properties for a DRS. They can be modelled in Tamarin using first-order logic. The requirement of cash for container can be modelled as

```
lemma CashForContainer:
"( All H1 value_I conts_I #k. H1GetFromH2(H1, value_I, conts_I)@k ==>
 (Ex conts_O conts_I #j. H1SendToV(H1, conts_O, conts_I)@j & j<k))
"
```

where `H1GetFromH2` and `H1SendToV` are labels for the rules that capture respectively step 9 and step 1 of the ceremony.

Similarly, the requirement of cash for voucher is captured by the following lemma

```
lemma CashForVoucher:
"( All H1 value_I conts_I #i. H1GetFromH2(H1, value_I, conts_I) @i ==>
 (Ex H2 SN1_I voucher_O #j.
  VSendToH1(H2, SN1_I, value_I,conts(conts_I), voucher_O) @ j & j<i))
"
```

The label `VSendToH1` corresponds to the rule in which the RVM prints the voucher (step 3).

Finally, the requirement of unique voucher can be modelled as

```
lemma UniqueVoucher:
"( All H2 voucher valid1 valid2 money value H2_2
   valid1_2 valid2_2 money_2 value_2 #i #j.
   H2SendToH1(H2, voucher, valid1, valid2, money, value)@i &
   H2SendToH1(H2_2, voucher, valid1_2, valid2_2, money_2, value_2)@j ==>
   #i=#j)
"
```

The label `H2SendToH1` captures the step in which the cashier hands the money to the customer (step 9). The terms `valid1` and `valid2` refer respectively to the successful validation signal that the cashier receives from the register and to the verification message that the server sends to the register. There is also a difference between `money` intended as coins and banknotes, and the piece of information regarding their `value`. Note that all the parameters of the two labels but `voucher` are different. The temporal marks `i` and `j` are crucial: if step 9 is executed twice with the same voucher, it should be referring to the same action, that is, all the parameters have indeed the same values.

In Table 2 are the results obtained by checking the ceremonies in Tamarin. Concerning the ceremonies at Kvickly and Coop stores, the tool proves that the ceremony with aware humans meets cash for container and cash for voucher. The requirement of unique voucher is not met because two different RVMs print the same SN1 barcode as this depends on the number of containers filled by the customer. Tamarin finds attacks for all three properties when inattentive

Table 2: The result of the ceremony analysis of the Danish DRS

	Kvickly & Coop			Netto		
	Aware	Inattentive	Unaware	Aware	Inattentive	Unaware
Cash for container	✓	✗	✓	✓	✗	✓
Cash for voucher	✓	✗	✗	✓	✗	✓
Unique voucher	✗	✗	✗	✓	✓	✓

customer actions are considered as part of the ceremony. We found that the common issue that leads to falsify the properties is that the attacker may create fake vouchers based on what he has seen earlier. Namely, the attacker can create vouchers that were never printed by any RVM. This is also possible because the attacker knows that the SN1 only depends on the number of containers. For the same reason, the ceremonies at Kvickly and Coop stores fail at ensuring cash for voucher when actions from unaware cashier are considered: the Tamarin trace shows that the attacker can just hand the voucher to the cashier a second time if the latter does not destroy it properly. Notably, the attack is possible even if the vouchers are synced and controlled through the Tomra servers, as the voucher is based solely on the number of containers filled in by customers. It is enough that a number of customers have filled in the same number of container, for the Tomra servers have multiple vouchers with the same SN1.

The DRS ceremony for the Netto stores meets all the requirements when aware humans are considered. However, if one considers an inattentive customer, cash for container and cash for voucher cannot be ensured. This is because the attacker, once he knows the SN1, can print the voucher on its own and be refunded in place of the legitimate customer. However, both cash for container and cash for voucher are met for unaware cashier since the SN1 are uniquely generated and, once they are redeemed, the Tomra servers remove the SN1 from the list of valid barcodes, making it impossible for an attacker to redeem the corresponding vouchers again. The requirement of unique voucher is met in all scenarios. However, Tamarin cannot prove unique voucher for unaware cashier if the Tomra server sends only an acknowledgement about the validity of a specific voucher. We found that it is required that the server explicitly sends back the valid SN1 to the cash register, and the latter checks the correctness of this against the scanned voucher.

4.1 Discussion

Having analysed formally the ceremonies for the Danish DRS, we can conclude that, according to our model, the Kvickly and Coop ceremony is less secure than the one in Netto stores. The main problem with that ceremony is that one can generate a voucher by guessing the number of containers that other customers may have previously filled into any of the RVMs that belong to the supermarket chain. This is worsened by the fact that vouchers have the same SN1

independently from which RVM they have been generated, hence an attacker can likely be successful on redeeming a fake voucher holding the same SN1.

The Netto ceremony sees the RVMs generating the SN1 based on an internal counter. Thus, each voucher is unique and is validated against a check with the Tomra servers. The Netto ceremony is secure in all scenarios but inattentive customers. However, we analysed the ceremony assuming that the attacker has no access to the internal counter of an RVM. Hence, the Netto ceremony is potentially vulnerable if one knows the current counter of an RVM. We believe that such potential vulnerability can be easily removed by using digital signatures, which would make the vouchers not predictable any more. The presence of digital signatures in paper ticketing has been already developed in public transportation. The signatures are generated by the public transportation server, encoded as QR codes, and then scanned by the ticket inspectors who hold portable scanners that store the verification key [4]. The Danish deposit return system can be modelled in a similar way. The voucher can be signed by the RVM, while the cash register can store the verification key. Since the digital signature of an SN1 cannot be forged, vouchers cannot be fully predicted by the attacker unless he knows the signing key. We modelled the Netto ceremony with digital signatures in Tamarin and the outcome of our analysis confirms that the ceremony would meet at least the same level of security of the original Netto ceremony. However, in the case of inattentive customers, an attacker can still make a copy of a voucher and redeem them in place of the customer. We believe that this attack cannot be avoided unless the customer is actively involved in the generation and validation of the voucher, for example using a PIN.

5 Related Work

Formal approaches for the analysis of socio-technical systems have been recently proposed in a few works. Basin et al. [1] formalised models of humans in security protocols and analysed two-factor authentication protocols in Tamarin as case studies. They considered three main human models. The first is the *infallible human* model, in which the human actions follow the prescribed steps of the protocol. In this paper, it corresponds to the aware humans. The second model is the *untrained human*, in which the human actions are completely controlled by the Dolev-Yao attacker. The last model is the *rule-based human*, which is defined as the untrained human with specific restricting rules that limit the arbitrary behaviour of the Dolev-Yao attacker. Conversely, this paper models the inattentive customer and unaware cashier actions as rules that extend the canonical description of the ceremony.

Johansen and Jösang [5] discussed probabilistic models of humans, while Probst et al. [14] proposed novel formal approaches to analysing socio-technical systems. Bella and Coles-Kemp [2] provided a model for the analysis of security ceremonies termed *the ceremony concertina* and demonstrated it by formally analysing the Amazon user registration ceremony using the Inductive Approach [13]. Giustolisi et al. [15] analysed the TLS certificate validation in different

browsers in front of socio-technical properties using UML and model checking tools. Stojkovski et al. [18] recently proposed a model to define socio-technical misalignments between a technical system and its users, and formally verified an end-to-end email encryption system against a set of misalignment properties. Differently from the works outlined above, which consider a single human role, this paper provides a formal account on human-to-human interactions as it considers a ceremony with customers and cashiers.

Martina et al. [9] and more recently Martimiano and Martina [8] proposed a shift from the classical Dolev-Yao attacker model to a more dynamic and human-centred threat model. In this paper, we still rely on the Tamarin built-in Dolev-Yao attacker, although we believe that the analysis of our case study into a different threat model may be beneficial to gain even more accurate and deep understanding of the security of the ceremony.

6 Conclusion

This paper has shown that the socio-technical analysis of a security ceremony can be pivoted on field observation and formal verification tools. Field observation enables the reverse engineering of ceremonies, as they usually lack proper documentation. Thus, field observation produces a specification that can be fed into a formal verification tool. The latter provides a precise way to dissect the security implications of the ceremony and allows one to formulate and verify potential mitigations.

To the best of our knowledge, this paper has provided the first security analysis of a DRS considering its human players. Although DRS is a well-established technology in Denmark and other countries in the world, it has been found that RVM manufactures devote most of their efforts to the detection of fake containers rather than detecting the refunding of fake vouchers. This work has also found that minor changes in the technology behind DRS may lead to severe security implications, although the technology comes from the same manufacturer and human interactions are identical. Fixing the technology to cope with the behavioural actions that people may perform outside the box is yet an open problem. Other countries adopt a voucher-less scheme in which customers are provided with personal cards. Customers use their cards to collect points that can be redeemed for rewards. While personal cards may mitigate threats due to inattentive customers, they pose novel privacy threats by exposing customers' habits in purchasing cans and bottles. We are not aware whether the findings of this work are applicable to other manufacturers and countries. We have contacted both Dansk Retursystem and Tomra on the issue and, at the time of writing this paper, we are waiting for a reply.

This work aims at contributing to the establishment of holistic approaches to security. Future work should focus on how systematically model out-of-the-box human interactions into behavioural actions that can be fed into a formal verification tool. A desirable feature of such a model is to make it independent from the specific ceremony so that it would be possible to build a formal framework

for the analysis of less restricted security ceremony. As regards the analysis of DRS, we believe that it would be interesting to investigate other scenarios such as the one with additional behavioural actions as well as analysing the implications of scenarios with multiple behavioural actions from different people at the same time. However, the Dolev-Yao attacker may be too powerful to appreciate the subtleties entailed by such scenarios, hence we think that a different threat model than the Dolev-Yao attacker should be considered. Finally, it would be interesting to analyse recent voucher-less and fully digital DRS proposals in which customers receive their refunds using an app [19]. The more pervasive the technology becomes, the more socio-technical analysis is required.

References

1. Basin, D., Radomirovic, S., Schmid, L.: Modeling human errors in security protocols. In: 2016 IEEE 29th Computer Security Foundations Symposium (CSF). pp. 325–340 (June 2016)
2. Bella, G., Coles-Kemp, L.: Layered analysis of security ceremonies. In: 27th IFIP SEC 2012. pp. 273–286. Springer, Berlin, Heidelberg (2012)
3. Ellison, C.: Ceremony design and analysis. IACR eprint (2007)
4. Giustolisi, R.: Free Rides in Denmark: Lessons from Improperly Generated Mobile Transport Tickets. In: The 22nd Nordic Conference on Secure IT Systems. pp. 159–174. Springer International Publishing, Cham (2017)
5. Johansen, C., Jøsang, A.: Probabilistic modelling of humans in security ceremonies. In: 3rd International Workshop on Quantitative Aspects in Security Assurance (QASA 2014). pp. 277–292. Springer (2015)
6. Jorgensen, A.: Method, system, reverse vending machine and use thereof for handling empty packaging (11 2005), `https://patents.google.com/patent/US20050246225A1/en`, US20050246225A1
7. Kavli, T.O., Njastad, J., Saether, G.: Method and apparatus for detecting fraud attempts in reverse vending machines (11 2012), `https://patents.google.com/patent/US9189911`, US9189911B2
8. Martimiano, T., Martina, J.E.: Daemones non operantur nisi per artem. In: Security Protocols XXVI. pp. 96–105. Springer International Publishing, Cham (2018)
9. Martina, J.E., dos Santos, E., Carlos, M.C., Price, G., Custódio, R.F.: An adaptive threat model for security ceremonies. International Journal of Information Security **14**(2), 103–121 (Apr 2015)
10. Meier, S., Schmidt, B., Cremers, C., Basin, D.: The tamarin prover for the symbolic analysis of security protocols. In: Sharygina, N., Veith, H. (eds.) Computer Aided Verification. pp. 696–701. Springer Berlin Heidelberg, Berlin, Heidelberg (2013)
11. Müller, H.A., Jahnke, J.H., Smith, D.B., Storey, M.A., Tilley, S.R., Wong, K.: Reverse engineering: A roadmap. In: Proceedings of the Conference on The Future of Software Engineering. pp. 47–60. ICSE '00, ACM, New York, NY, USA (2000)
12. Nordbryhn, A., Hansen, A.H.H.: Fraud detection (02 2019), `https://patents.google.com/patent/EP3440641A1/en`, EP3440641A1
13. Paulson, L.C.: The inductive approach to verifying cryptographic protocols. J. Comput. Secur. **6**(1-2), 85–128 (Jan 1998)
14. Probst, C.W., Kammüller, F., Hansen, R.R.: Formal modelling and analysis of socio-technical systems. In: Semantics, Logics, and Calculi: Essays Dedicated to

Hanne Riis Nielson and Flemming Nielson on the Occasion of Their 60th Birthdays. pp. 54–73. Springer (2016)
15. R.Giustolisi, Bella, G., G.Lenzini: Invalid Certificates in Modern Browsers: A Socio-Technical Analysis. IOS Journal of Computer Security **26**(4), 509–541 (2018)
16. Saether, G.: Means in a reverse vending machine (rvm) for receiving, handling, sorting and storing returnable items or objects (07 2010), https://patents.google.com/patent/US7754990B2/en, US7754990B2
17. Saether, G., Sivertsen, R., Lunde, T., Njastad, J.: Fraud detection system and method (08 2018), https://patents.google.com/patent/US20180232745A1/en, US20180232745A1
18. Stojkovski, B., Vazquez Sandoval, I., Lenzini, G.: Detecting misalignments between system security and user perceptions: a preliminary socio-technical analysis of an e2e email encryption system. In: 4th European Workshop on Usable Security (2019)
19. Tomra Systems Asa: myTOMRA app. https://www.mytomra.com.au/home/the-mytomra-app/, accessed 05-July-2019
20. Tomra Systems Asa: Voucher control. https://www.tomra.com/en/collection/reverse-vending/tcs-digital/voucher-control, accessed 05-July-2019