Free Rides in Denmark: Lessons from Improperly Generated Mobile Transport Tickets

Rosario Giustolisi(✉)

IT University of Copenhagen, Copenhagen, Denmark
rosg@itu.dk

Abstract. The term *security ceremony* describes a technical system extended with its human users. In this paper, we examine the inspection ceremony for the mobile transport ticket in Denmark. We find several security weaknesses that are ascribable to both human and computer components of the ceremony. The main vulnerabilities are due to the design choices of how the visual inspection ceremony is organised and the lack of information that is stored into the 2D barcode. These vulnerabilities allow a ticket holder to travel up to 8 zones with a 2-zone subscription and enable several people to travel with the same subscription. The attack is significant as it can be automated, and rather modest skills are necessary to break the inspection ceremony. We state four principles that aim at strengthening the security of inspection ceremonies and propose an alternative ceremony whose design is driven by the stated principles.

1 Introduction

Denmark has a modern transport infrastructure. The Danish government has recently allocated substantial investments in infrastructure for railways, buses and new metro lines [1]. Copenhagen, the capital with just over 700,000 inhabitants, has one of the most advanced metro systems in the world that runs autonomously 24 h a day. Approximately one million people use the metro every week [2]. Several transportation companies operate bus, metro, and train services sharing the same ticketing system. Travellers can purchase three different ticket formats: paper, contactless smart card, and digital app. Each ticket format has its purchase and inspection procedures.

Travellers can purchase season tickets in digital format through a smartphone app, which in Danish is called *Mobilpendlerkort*. The app enables commuters to buy a digital subscription for a 30 up to 183 days in adjacent travel zones in Denmark. Season tickets allow commuters to take advantage of unlimited trips on buses, trains and metro for a discounted price. Hence, they are personal and should be used only by the person who is registered as the user in the app.

Introducing new payment technologies goes hand in hand with designing the corresponding process to check the validity of a ticket. There are many different ways of how such a process could be organised. London transit, for example,

H. Lipmaa et al. (Eds.): NordSec 2017, LNCS 10674, pp. 159–174, 2017.
https://doi.org/10.1007/978-3-319-70290-2_10

has introduced the Oyster card, which is physically checked upon entering and before leaving buses or stations. In Denmark, the solution is different. Train guards are going around and checking the validity of the tickets. In long distance trains, every customer is asked to provide a ticket, in local trains and Metro trains inspections occur often, and in buses, inspections are permitted but rarely happen at all, although one has to display the proof of purchase to the bus driver before entering. Also, new mobile payment technologies brings along new challenges of adjusting existing and designing new ticket inspection ceremonies. Nowadays, the inspection ceremony must also work for digital tickets including those printed on paper or displayed on a mobile phone's screen. Inspectors may use barcode scanning technology or use other means to assess the validity of a ticket.

In this paper, we investigate the security ceremony that involves the inspection of the mobile transport tickets. According to Ellison [3], the term *ceremony* refers to a technical system extended with its human users. Security ceremony analysis, also known as socio-technical security analysis, is an area of research that has been initiated only recently although it is widely accepted that security incidents usually bootstrap from social engineering practices. Those practices target the weakest link in the security chain, namely, the user. The idea behind the socio-technical security analysis is to combine computer security and social sciences into an interdisciplinary approach that brings the human in the context of information security analysis. Recently, a socio-technical attack has been carried out against UK rail tickets [4]. BBC reporters bought forged rail tickets on the dark web. Although the tickets appeared genuine, magnetic strips were not accepted by the barriers. However, train guards let BBC reporters through the barriers at all occasions without asking any questions.

In a similar vein, we conduct our security analysis considering both human and computer components involved in the inspection ceremony. Our findings include an attack, which would allow a malicious commuter to exploit weaknesses in the app and the inspection ceremony to ride trains, buses, and metro in Denmark for free. If carefully orchestrated, the attack can elude post-processing inspection analysis attempting to detect fraudulent activities and may affect railway companies: the prices of a personal season ticket range from a minimum of 375 kroner (50 euros), for one month covering 2 zones, to a maximum of 32099 kroner (4315 euros), for three months covering 28 zones in first class. The cost depends on multiple factors such as period, travel class, the number of travel zones, and type of ticket. Our work in this paper makes the following contributions:

- We detail the security analysis of the inspection ceremony of digital season tickets and reports some security weaknesses that enable a concrete attack to the ceremony. Since there are no publicly available specifications of the ceremony, we build the ceremony via a three-phase analysis (observation, interaction, validation) of the procedures that train guards follow during an inspection. For a similar reason, we decode the barcode printed into the Mobilpendlerkort to gain the encoded data.

- We advance four principles to transport operators aimed at improving the security design of the tickets. We formulate our principles on the basis of the outcome of our ceremony analysis and findings. It follows that the principles are specifically devised for the ticket inspection ceremony but can be further generalised and applied to other socio-technical contexts.
- We propose an alternative inspection ceremony that is aimed at strengthening the security of the inspection procedure. The design of the alternative ceremony is driven by our principles. While it provides stronger security guarantees, it is simpler than the original ceremony.

Outline. Section 2 describes the Mobilpendlerkort app and the inspection ceremony; Sect. 3 details the steps that enable the attack to the ceremony; Sect. 4 outlines four principles for the design of ticket inspection ceremony; Sect. 5 details an alternative ceremony that mitigates the attack in the original one; Sect. 6 discusses related work; finally, Sect. 7 concludes the paper.

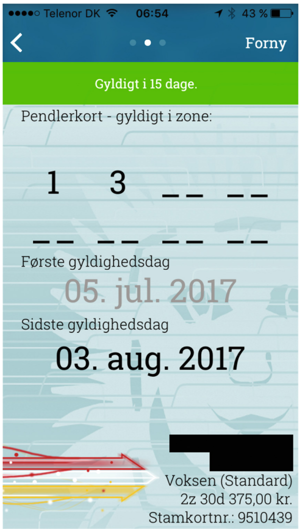
2 Ceremony Description

The inspection ceremony is pivoted on the elements provided by the Mobilpendlerkort app and on how the train guard interprets these elements. The user installs the app and purchases a season ticket. The train guard is expected to execute the inspection ceremony according to the details of the season ticket available in the app.

2.1 Description of Mobilpendlerkort

The Mobilpendlekort app is available for mobile devices running iOS or Android operating systems. It is published by *DSB*, the largest train operating company in Scandinavia. We consider the latest available version (3.01) that is available at the time of writing this paper. Both iOS and Android versions of the Mobilpendlerkort implement the same functionalities. Hence, the security issues and the principles later described in this paper apply to both versions of the app.

Once the app is installed, it requires the commuter to enter the mobile phone number. The app generates a subscription number (*stamkortnr*) that is bound to both device and phone number. If the commuter changes device or phone number, the app generates a new subscription number, hence former season ticket cannot be restored, and the commuter should purchase a new season ticket. To purchase a season ticket, the commuter provides her personal details (i.e., name, surname, and birth date), chooses the starting and ending dates, and the desired travel zones. After payment, the app downloads and installs the ticket, which is represented via two screens. The *primary* screen is intended for visual inspection and includes an animated visual watermark. The *secondary* screen is intended for computer inspection and includes a 2D barcode that encodes a digital signature on the ticket data. An instance of a valid ticket is depicted in Figs. 1 and 2, which show the primary and secondary screens, respectively.



●●●●○ Telenor DK 06:54 43 %

Forny

Gyldigt i 15 dage.

Pendlerkort - gyldigt i zone:

1 3 __ __

__ __ __ __

Første gyldighedsdag

05. jul. 2017

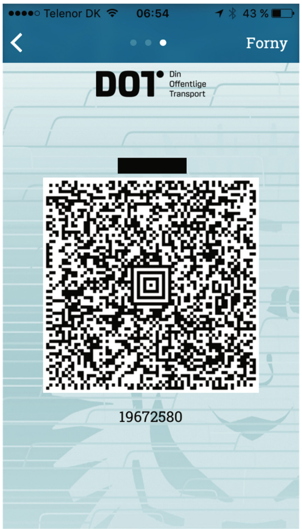
Sidste gyldighedsdag

03. aug. 2017

[redacted]

Voksen (Standard)
2z 30d 375,00 kr.
Stamkortnr.: 9510439

Fig. 1. A screenshot of the primary screen (personal details are hidden)



●●●●○ Telenor DK 06:54 43 %

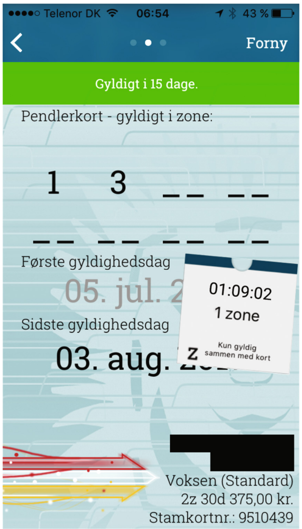
Forny

DOT Din Offentlige Transport

[redacted]

19672580

Fig. 2. A screenshot of the secondary screen



●●●●○ Telenor DK 06:54 43 %

Forny

Gyldigt i 15 dage.

Pendlerkort - gyldigt i zone:

1 3 __ __

__ __ __ __

Første gyldighedsdag

05. jul. 2

Sidste gyldighedsdag

03. aug.

01:09:02
1 zone
Z Kun gyldig sammen med kort

[redacted]

Voksen (Standard)
2z 30d 375,00 kr.
Stamkortnr.: 9510439

Fig. 3. A screenshot of the primary screen with an extra zone ticket

The center of the primary screen displays the valid travel zones and the time interval for which the ticket is valid. In the lower-right corner, the screen displays the personal details of the commuter, the type of the ticket (i.e., young, adult, or senior), the number of zones and the number of days included in the subscription, the purchase price, and the subscription number. In the lower-left area of the primary screen there is the animated visual watermark that is intended to provide visual assurance about the authenticity of the app. The secondary screen displays the phone number of the commuter, the ticket number, and a 2D barcode, specifically an Aztec type of barcode, which is the *de facto* standard for mobile transport tickets. A new ticket number is generated whenever the subscription is renewed. The Aztec barcode contains most of the data displayed on the primary screen and the respective digital signature. Section 3 provides a detailed description of the content of the barcode.

The app also allows commuters to purchase additional extra zone tickets that extend the number of travel zones temporarily. Extra zone tickets are visually *stapled* on the primary screen. For instance, the extra zone ticket in Fig. 3 allows the commuter to travel to one additional zone, namely, any of the zones that are adjacent to the zones already included in the subscription. It is possible to purchase extra zone tickets for up to 8 additional zones.

2.2 Building the Inspection Ceremony

There is no available public specification for the inspection ceremony of transport tickets in Denmark. Thus, we derived the steps that form the ceremony empirically. The procedure to build the ceremony included three phases. In the *observation* phase, we observed how train guards interact with the app, either when a valid or invalid ticket (i.e., expired, with wrong zones or personal details) is checked. We noted the behaviours of train guards on metro and trains in the Copenhagen metropolitan area. On buses, we observed the inspection done by bus drivers. The output of this phase was a preliminary draft version of the ceremony. The draft served as input to the *interaction* phase in which we interacted with train guards to refine the structure of the ceremony when they checked our valid tickets. For example, we asked the train guard to execute a full inspection. We found that the inspection ceremony varies according to the mean of transport and the cost of the ticket. For example, guards on metro and buses are not equipped with scanners that can check barcodes, hence those guards can only proceed with the visual inspection. Also, we realised that guards check ID documents on metro rides either randomly or if they believe that the personal details displayed on the primary screen of the app do not match with the mobile phone holder (e.g., the app reports a typical female first name but the holder is a male). Then, we moved to the *validation* phase, in which we asked the IT security department at DSB to confirm about the correctness of the ceremony. DSB personnel confirmed that steps outlined in the ceremony are correct, while they preferred not to comment whether the ceremony comprises other steps that we have not observed empirically. More details about DSB response are outlined in Sect. 4.

Figure 4 summarises the various steps required for mobile ticket inspection, which unfolds as follows. Upon request of the train guard, the commuter shows the primary screen of the ticket along with an authentic and valid ID document. The train guard visually checks the authenticity of the primary screen provided by the animated visual watermark, image background, and font of the text. The train guard then checks the validity of dates and zones reported on the ticket. For short rides, such as metro rides, or in rush hours, the train guard may decide to conclude the inspection and consider the ticket valid. Earlier successful conclusions of the ceremony are depicted with dashed lines in Fig. 4. Otherwise, the train guard may check that the personal details of the ID document match name, surname, and birth date reported in the primary screen. During the last step of the inspection ceremony, the train guard checks the validity of the barcode using an hand-held scanner, which is equipped with the verification key to validate the signature. The device emits a green light if the verification is successful and a red light otherwise.

It is clear that ticket inspection is a socio-technical procedure as it involves actions and decisions from both human and computer components. It follows that the security of such procedure depends on elements ascribable to human users (i.e., the train guard), computer technology (i.e. the app and the scanner), and the interaction among them. As we shall see later, this observation is important

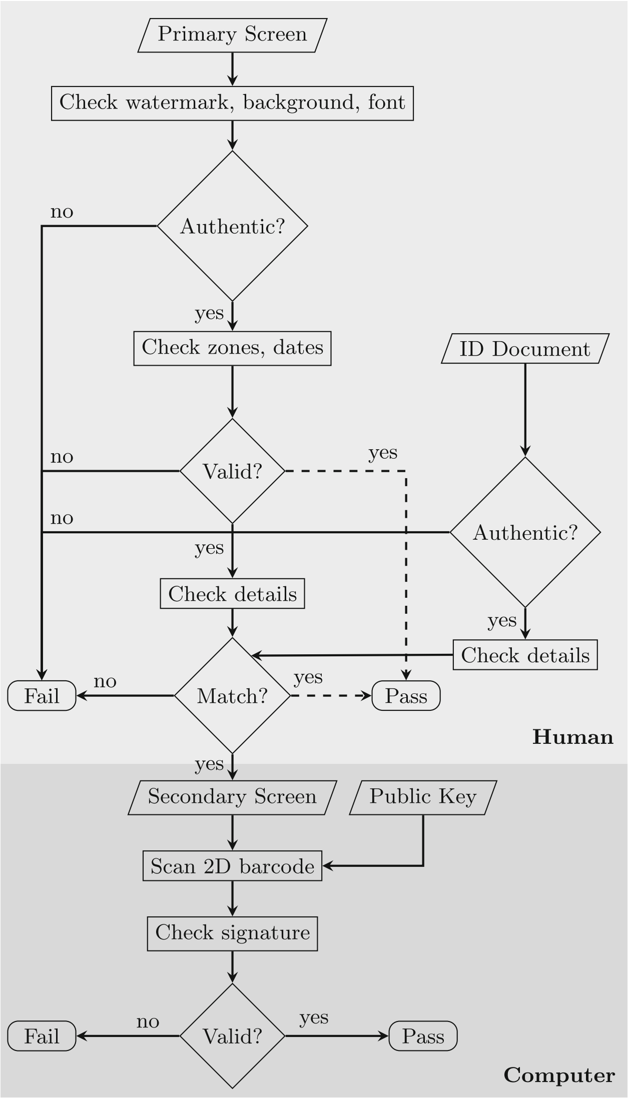


Fig. 4. The inspection ceremony executed by the train guard

as it leads to the finding of security weaknesses and provides grounds for the security principles.

3 Attack Demonstration

This section describes an attack that exploits the security weaknesses of the inspection ceremony. To describe the attack, we first report the procedure leading to evidence of weaknesses on the generation of the barcode. Then, we discuss how to forge the primary screen to break the inspection ceremony by combining the forged primary screen with the barcode.

```
23 55 54 30 31 31 31 38  36 30 30 30 30 31 30 2c  |#UT011186000010,|
02 14 6d 48 6c 80 cb 75  95 79 58 bc 92 6a 8f 9b  |..mHl..u.yX..j..|
f7 ee 04 5d f8 7b 02 14  1c ad fe ef 43 4a 84 1c  |...].{......CJ..|
4d ce 94 7a 18 6c 7b 55  ba 4a c5 c6 00 00 00 00  |M..z.l{U.J......|
30 32 37 35 78 da 65 91  cd 4e c3 40 0c 84 5f 65  |0275x.e..N.@.._e|
cf 55 a9 c6 fb e3 dd e4  80 54 9a a8 54 e9 a1 a2  |.U.......T..T...|
e9 a1 5c aa 48 c9 81 4b  40 81 f7 17 76 8a c2 22  |....H..K@...v.."|
7c fb 6c cf 78 b2 b9 dc  9e eb 6d 05 02 82 23 4a  ||.l.x.....m...#J|
4c d1 c7 00 07 93 15 a4  61 41 91 6c 48 be ef 86  |L.......aA.lH...|
f1 72 6b 8f db ab 88 7c  e1 5e 76 ad 05 6c 04 84  |.rk....|.^v..l..|
49 94 52 ae 3a 3f 09 26  10 91 f6 e9 fc d5 8d 7d  |I.R.:?.&.......}|
37 f5 e6 54 0b 49 1f ac  7b dc 1e 76 4d dd c2 ca  |7..T.I..{..vM...|
05 31 d3 96 d7 10 e2 22  5e 64 55 6b f7 d7 63 75  |.1....."^dUk..cu|
d8 97 46 13 40 12 c8 28  e8 a6 48 cc c7 20 46 b4  |..F.@..(..H.. F.|
9c 01 6f e0 0c 50 aa 77  b0 4b 9f fc 06 de 80 b4  |..o..P.w.K......|
1f 83 9f 83 ea 60 85 78  3f b5 50 91 13 23 23 26  |.....`.x?.P..##&|
dd 2c 94 8a d7 f7 71 30  a4 d3 48 b9 9e f5 99 a0  |.,....q0..H.....|
b1 61 1f 1e 11 ff 22 3b  ff cf c1 c9 52 9e 87 39  |.a....";....R..9|
2d 64 25 41 ca 66 29 fb  52 d5 4f a5 a1 b5 71 bf  |-d%A.f).R.O...q.|
99 e7 5f 90 03 e5 30 67  09 3f e0 f4 75 c4 51 2a  |.._...0g.?..u.Q*|
9d a6 b7 4f 53 35 0d 39  d6 03 77 9b 95 94 4f 69  |...OS5.9..w...Oi|
0d 7c 03 b6 cf 72 04                              |.|...r.|
```

Fig. 5. Raw data encoded in the 2D barcode. The sequence `302c 0214` reveals the header of the signature. The sequence `78da` reveals the header of a compressed payload.

3.1 Barcode Analysis

The first step for the analysis of the barcode content is to get the raw data codified in the barcode. There are many barcode decoders available on the Internet that can recover data from barcodes, e.g., ZXing, WebQR. Figure 5 shows the raw data encoded in the barcode contained in the secondary screen of Fig. 2. The first 14 bytes are reserved for the header of the ticket. The presence of the string "*#UT*" in the header confirms that the structure of the barcode follows the UIC 918-3 standard [5], which prescribes the use of public key cryptography. Information about the verification keys used by DSB and most popular train operators in Europe are publicly available for download [6]. The header is followed by a digital signature that is generated using DSA-SHA1 (1024-160).

Most of the data encoded in the barcode is the payload, which is compressed into zlib format. Since only the content of the payload is signed, it is important that it contains as much information as possible about the ticket to prevent its forgery.

Since the structure of digital tickets is not open source, we derived it using a differential analysis approach. We purchased different season tickets and studied how the respective payloads differ. In so doing, we were able to isolate the elements that form the structure of the digital ticket, for example, the purchase date, the price, etc. This approach led to an interesting finding. We considered two season tickets for the same travel zones but having different personal

```
U_HEAD0100531186 17475030 0503201712584daenU_TLAY010493RCT200270001010
300003DSB0018011100011Standard
PE0118010600006TICKET0205010400004118603010112000012GYLDIG:
2017025801050000501pe06010111000110 6.0300:00065201110001114.0401:
000754010100001*0703010100001*0709010100001*0760010100001
*0613010900009Zone10010713010100001*0632010200002->
0732010200002->0634010900009Zone 10030734010100001
*066801010000120768010100001*0801011100011Zoner: 1,
309010100000001001010000000110101000000012010250000001352010800008
Pris DKK1361011000010****488,00

U_HEAD0100531186 17641124 1303201721194daenU_TLAY010493RCT200270001010
300003DSB0018011100011Standard
PE0118010600006TICKET0205010400004118603010112000012GYLDIG:
2017025801050000501pe06010111000111 4.0300:00065201110001115.0401:
000754010100001*0703010100001*0709010100001*0760010100001
*0613010900009Zone 10010713010100001*0632010200002->
0732010200002->0634010900009Zone 10030734010100001
*066801010000120768010100001*0801011100011Zoner: 1,
309010100000001001010000000110101000000012010250000001352010800008
Pris DKK1361011000010****400,00
```

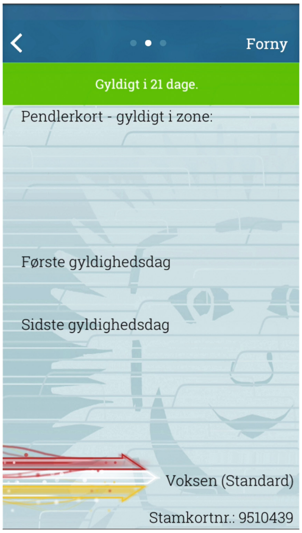
Fig. 6. The payload of the two tickets. The differences between the two payloads are in bold. There is no mention of the personal details of the commuters.

details, starting, and ending dates. We expected that the different key information between the tickets should be reflected on the payload. Figure 6 highlights the data of the two payloads. As expected, we found that the payload includes information about the ticket number, purchase date and time, ticket type, travel zones, and purchase price. Surprisingly, the personal details of the commuter cannot be found in the payload. This means that the authenticity of the personal details reported in the primary screen only relies on the unforgeability of that screen.

3.2 Primary Screen Forgery

The primary screen should be usable, namely the visual inspection should not take too long to evaluate the authenticity of the data reported on the screen. On the other hand, any alteration of the screen should be noticeable to the train guard at visual inspection. We note that the unforgeability of the primary screen mainly depends on fonts, the position of the text, background image, and animated visual watermark. As expected, the animation has complex elements that make the animation difficult to reproduce.

Unfortunately, the primary screen can be forged in few steps and, most importantly, once the background and the visual watermark are reproduced, the forgery can be automated. We observe that no text overlays the visual watermark, hence the latter can be obtained by recording a video of the primary screen on the phone (Quicktime can capture iPhone screens). Then, the resulting video can be converted into a GIF image to facilitate editing. We also observe that only name, surname, and birth date need to be edited because other information is sealed into the signature encoded in the barcode. It follows that only a small portion of the background needs to be edited and replaced with the desired



Gyldigt i 21 dage.

Pendlerkort - gyldigt i zone:

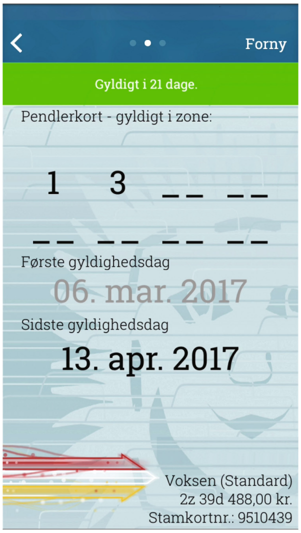
Første gyldighedsdag

Sidste gyldighedsdag

Voksen (Standard)

Stamkortnr.: 9510439

Fig. 7. A screenshot of a complete empty forged primary screen as template



Gyldigt i 21 dage.

Pendlerkort - gyldigt i zone:

1 3 __ __

__ __ __ __

Første gyldighedsdag

06. mar. 2017

Sidste gyldighedsdag

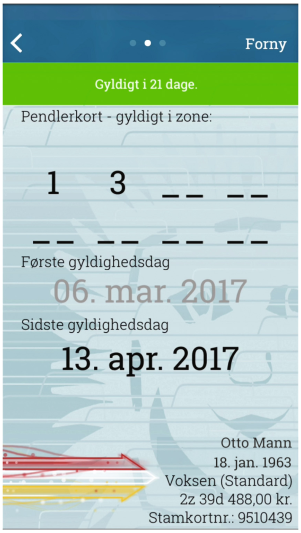
13. apr. 2017

Voksen (Standard)

2z 39d 488,00 kr.

Stamkortnr.: 9510439

Fig. 8. A screenshot of the forged primary screen as template



Gyldigt i 21 dage.

Pendlerkort - gyldigt i zone:

1 3 __ __

__ __ __ __

Første gyldighedsdag

06. mar. 2017

Sidste gyldighedsdag

13. apr. 2017

Otto Mann

18. jan. 1963

Voksen (Standard)

2z 39d 488,00 kr.

Stamkortnr.: 9510439

Fig. 9. A screenshot of the forged primary screen filled with a placeholder name

name, surname, and birth date, although a complete empty primary screen can be easily obtained (Fig. 7). This makes the forgery procedure even easier than expected: there is no need for a dedicated app, a GIF image is sufficient to make a successful forgery.

The last step needed to complete the forgery is to use the correct font. Any online font identifier can recognise the font, which in this case is *RobotoSlab Regular*. Figure 8 shows a screenshot of a forged primary screen that can be used as a template to create several primary screens with different personal details automatically. Figure 9 depicts the template filled with placeholder details.

The attack is carried out by combining the secondary screen with a forged primary screen. In fact, even if the train guard checks the ticket holder's ID document, she may end up accepting the forged digital ticket. The attack breaks the inspection ceremony in both its human and computer components. It takes advantage of poor security choices in the design of the primary screen breaking the visual inspection on the screen (human component). The attack exploits the naive generation of the signature encoded in the barcode to pass the electronic check (computer component) of the secondary screen.

One may note that post-processing systems will eventually identify the concurrent use of a forged digital ticket, and annul it. Still, a forged digital ticket can be successfully used at different times of the day by different people.

The attack is very effective if orchestrated carefully. A more sophisticated version would be to purchase a season ticket with many travel zones and take advantage of the reduced price due to the incremental discount rate. The ticket would be distributed among several commuters that travel to different zones. In this case, the forged digital ticket can be implemented into a dedicated app that allows users to report when a forged digital ticket is scanned. This sophisticated version would be particularly virulent: fraudsters can coordinate the issue of forged digital tickets, minimising the risk that post-processing systems identify the concurrent or suspicious use of the tickets.

3.3 Extra Zone Ticket Forgery

Forging the extra zone ticket is even easier than the primary screen as there is no need to forge the app at all in this case. Less than one person-day of effort was needed to make an Android *floating app* that overlaps the primary screen of the Mobilpendlerkort. A floating app is an application that opens in a window and floats over all other applications allowing multitasking on a device. A popular use of floating apps are the chat heads of messaging apps like Facebook Messenger. In our case, the floating app consists of a fake extra zone ticket with a countdown timer that simulates the remaining validity time of the ticket. Our app does not float freely but sticks to the primary screen.

The extra zone ticket forgery is effective because the barcode does not change when extra zone tickets are purchased and takes advantage of the poor security design of the ticket in the primary screen to attack the visual inspection (human component).

4 Principles

Upon the basis of our findings, we formulate four principles that form the foundation for our proposed solution. The first principle focuses on differences between paper and mobile tickets.

Principle 1. *The security design of paper tickets should not influence the security design of electronic tickets.*

Often, look and feel of traditional systems tend to be copied in their electronic counterpart. This is a natural design choice because it takes advantage of the preexisting familiarity that stakeholders have with the system: it minimises end-user confusion caused by the introduction of electronic components; it allows system developers to get immediate correctness feedback from a system they already know well. With a security take, this approach should be practised more cautiously, prioritising secure by design principles when possible. For instance, it is mistakenly believed that a digital animation image gives the same degree of authenticity to mobile tickets as watermarks give to paper tickets. In our setting, the forged digital ticket is a clear example of how a pre-existing (working) approach in the traditional system influences the electronic one negatively.

Principle 2. *Computer inspection should be prioritised over visual inspection.*

An immediate consequence of Principle 1 is that computer components should not be seen as add-ons that follow the traditional inspection ceremony. Train guards are used to that a successful visual inspection signifies that the ticket is valid. Habits are hard to eradicate, especially when traditional and electronic systems coexist, as in the case for transport tickets. The human-then-computer ceremony may lead train guards to execute only the traditional inspection ceremony and consider mobile tickets valid when they are not. Designing a computer-then-human ceremony would result in train guards to diverge from the traditional ceremony, fostering awareness of the different inspection ceremonies.

When possible, it is also advisable to intertwine human and computer components in the inspection ceremony. A closer look at the inspection ceremony in Fig. 4 reveals an additional issue due to the separation of human and computer components. The last check validates the signature of a payload that is unintelligible to the human because the payload is encoded as a 2D barcode. The payload may contain different data respect to the information reported in the primary screen, and the output of the scanner (i.e., green or red light) is not sufficient to the train guard to check whether the payload actually encodes the same data as in the primary screen.

Principle 3. *The inspection ceremony should enable the verification of ticket key information either electronically or manually.*

Maintaining information in electronic form has many advantages, such as quick and human-errorless ticket verification. However, it is necessary that all key information is considered for checking. Complete information may not be available due to intentional or unintentional computer malfunctions. For example, scanners may not work properly during the inspection. It is desirable that the inspection ceremony provides the strongest possible security guarantees to both electronic and manual verification procedures. For example, the ceremony would benefit from practices such as data redundancy and data duplication. Both practices prompt verification procedures to have access to the necessary data and would help to avoid weaknesses such as the exclusion of commuter personal details from the payload of the barcode.

Principle 4. *Security should be preferred over usability in the design of visual inspection of an electronic ticket.*

The rationales underlying this principle are twofold. First, it comes from the observation that a ticket is not a receipt. The goal of a transport ticket is to prove *to the train guard* that the holder has a certain right, while the goal of a receipt is to prove *to the holder* that ticketing system received the money. A common mistake is not to separate concerns, for example, separate tickets with receipts. The design of a ticket demands security and usability towards the train guard while the design of receipt focuses on usability towards the ticket holder. The effort in balancing those conflicting requirements may lead to compromises and may introduce security weaknesses, which can be easily avoided by designing ticket and receipt separately.

Secondly, electronic tickets are more suitable for computer inspection than visual inspection, hence it is easier to guarantee the security of the inspection via computer components rather than human components. The security of visual inspection cannot be taken for granted, and visual assurance elements should be carefully designed to maximise security, sacrificing usability if necessary. The following design advice list aims at maximising the security of visual inspection.

- Prefer complex, large, and dynamic visual watermarks over simple, small, and static ones to mitigate forgery.
- Superimpose critical information and visual watermark to prevent data alteration.
- Display the current time to ensure liveness.
- Display visual watermarks across the screens to evidence screen correlation.

Of course, the list contains elements that may negatively affect the usability of the ceremony. However, we observe that this is not a real issue since train guards are expected to be specifically trained to perform a visual inspection. This is an additional element in support of prioritising security over usability in the design of visual inspection.

5 Alternative Inspection Ceremony

We propose a new inspection ceremony inspired by the principles outlined above. Where possible, we reuse the components of the actual ceremony. We believe that the reuse of existing components will reduce the need of training for train guards, hence will favour a faster adoption of the new ceremony.

Figure 10 shows the steps of the alternative inspection ceremony. A main pillar of the alternative ceremony is to prioritise computer inspection over visual inspection, as advocated in Principle 2. The primary screen is replaced with a *barcode screen*, that contains the Aztec barcode, which should encode zones, dates, and personal details of the commuter. This enables the verification of all ticket key information electronically as suggested in Principle 3. The hand-held scanner checks the barcode and, if the signature is valid, it shows the content of the payload (i.e., zones, dates, and personal details) on the screen of the scanner. The train guard now checks the validity of zones and dates by looking at the screen of the scanner. The last step consists of checking whether the personal details displayed on the screen of the scanner match with the details reported on the ID document.

The proposed inspection ceremony is simpler than the original one. The app needs only one screen to represent the ticket. This is possible by taking advantage of the screen on the scanner. The visual inspection now takes place on a device controlled by transport companies rather than on the commuter's device, which provides only the elements for computer inspection. Thus, the alternative inspection ceremony minimises the attack surface due to forged digital tickets

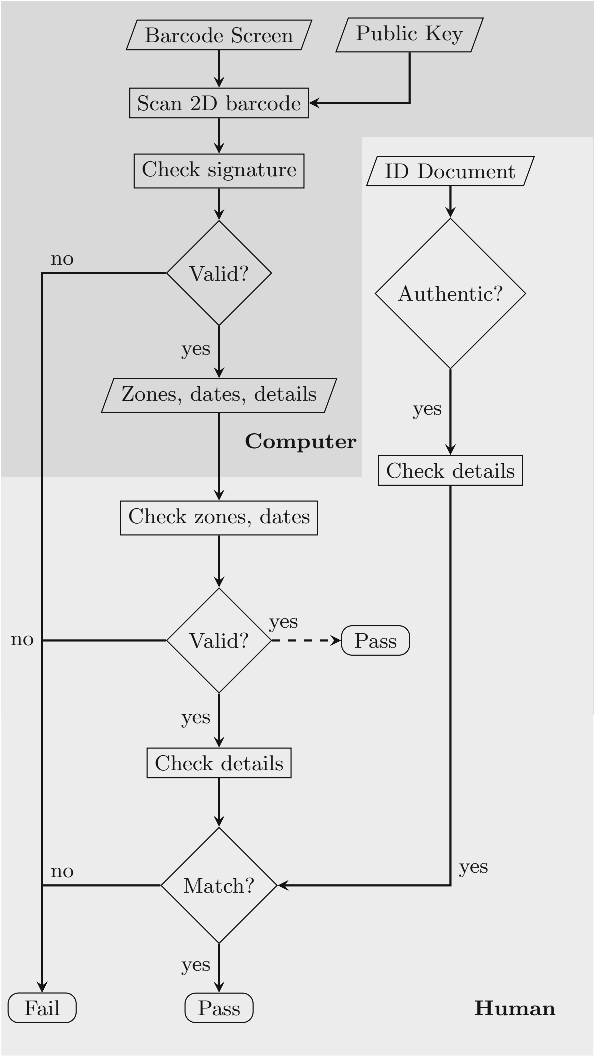


Fig. 10. The proposed inspection ceremony

on the human visual inspection. The proposed design provides more security guarantees in case of an earlier successful conclusion of the ceremony. The scanner does not emit light to signal the outcome of the verification anymore, hence the train guard needs to validate travel zones and dates, whose authenticity is provided by the digital signature encoded in the barcode. Although an earlier successful conclusion of the proposed ceremony does not ensure that the holder has the right to travel with that digital ticket, it still guarantees that the ticket is valid. Conversely, an early successful conclusion of the original ceremony does not give any guarantees about the validity digital ticket, which might be forged. An additional element in support of the proposed inspection is that it helps the post-processing analysis as each ticket inspection entails ticket scanning. The device can store the data collected on each scan, which is eventually sent to the post-processing systems as it happens with tickets in the form of contactless smart cards.

A secondary screen might still be necessary in the event that an hand-held scanner is unavailable. The animation image displayed on that screen should be replaced by a more robust form of digital watermark as suggested by the elements listed in Principle 1. It is important to stress that the ceremony should lead the train guard to look at this screen only under exceptional circumstances. This justifies the use of a more sophisticated and secure form of digital watermark at the cost of a slower visual inspection. The security of the alternative inspection ceremony is not proven, and it would be interesting to use formal approaches to appreciate the security of both original and proposed ceremonies.

Responsible Disclosure. We notified DSB as soon as we completed the security analysis of the inspection ceremony and found the security weaknesses. DSB examined our report and started reviewing the Mobilpendlerkort app. However, at the time of writing this paper, no new version of the app has been released. While DSB personnel confirmed that all the steps depicted in the inspection ceremony are correct, they preferred not to comment whether the ceremony comprises other steps that we have not observed empirically. For example, we would have been interested to know whether the scanner can remotely check a ticket online. If so, it is essential to know what data is exchanged between the scanner and the remote server. The presence of the digital signature into the barcode suggests that the scanner makes an offline check.

6 Related Work

Ceremony analysis has been increasingly studied as a way to better understand the security issues of real-world systems. Radke et al. [7] investigated strengths and weaknesses of ceremony analysis. Bella and Coles-Kemp [8] advanced a model in support of the socio-technical analysis of security termed *the ceremony concertina*. Johansen and Jøsang [9] proposed a probabilistic modelling of humans based on the ceremony concertina. Probst et al. [10] have recently discussed different approaches to modelling and analysing socio-technical systems formally. In our case, the approach to the ceremony analysis is informal. However, we believe that our case study would benefit from formal approaches and that new security issues might be found.

Garcia et al. [11] reverse engineered and made a cryptoanalysis of the MIFARE Classic card, a major player in contactless smart card market, with a strong presence in public transport systems. They found two attacks that allowed an intruder to get the secret key of a card. MIFARE Classic card could be cloned in under a second. Differently from our work, they exploit a security vulnerability of the cryptographic primitive of the authentication protocol. Murdoch et al. [12] attacked "Chip and Pin" cards issued by the EMV (Europay, MasterCard, Visa) consortium. They were able to make a successful transaction with a stolen card without knowing the PIN. They exploited the fact that the PIN verification step is never explicitly authenticated. In so doing, they were able to build a man-in-the-middle attack using a few hardware components and a fake card.

E-ticketing insecurity traces back to Schneier [13], which explained how easy was to fly on someone else's ticket by changing the name on the e-ticket boarding pass printed out at home. More recently, Jaroszewski [14] created a fake boarding pass app to enter airline lounges. Instead of generating the boarding pass, the app generates a barcode that is based on the flight number, and that can then be scanned at the entrance to lounges. The fake barcode worked because it was generated without any cryptographic authentication mechanism so unmanned automatic scanners could not check properly the eligibility of the passenger. This case is complementary to the case studied in our paper in which the involvement of human user (i.e., the train guard) might be harmful to the security of the system.

7 Conclusions

The socio-technical approach to the security analysis allowed us to find the security weaknesses that lead to the attacks. The contribution of this work is not in the attacks that we have identified but in the principles we have derived from our observation for the design of security ceremony. Building a security ceremony is not a straightforward task. There is no standard notation or known guideline that prescribes the right formalism to represent the flow of information in a security ceremony. The presence of human users further complicates the construction of the ceremony. In our case, we decided to use flowcharts because they provide a simple and clear graphical description, and naturally describe the heterogeneous protocol where users and computers are the players. The presence of the human component also complicates the design of a security ceremony. Human users tend to take shortcuts as in the case of earlier successful conclusions of the ceremony. With a security take, the shortcuts should be reduced as much as possible and, ideally, eradicated.

Acknowledgement. This work is supported in part by DemTech grant 10-092309 from the Danish Council for Strategic Research, Programme Commission on Strategic Growth Technologies.

References

1. Ministry of Transport of Denmark: Danish infrastructure investments (2012). https://goo.gl/irpQQR
2. Ministry of Foreign Affairs of Denmark: Transport infrastructure in Denmark (2012). http://denmark.dk/en/practical-info/work-in-denmark/transport-infrastructure-in-denmark

3. Ellison, C.: Ceremony design and analysis. IACR eprint (2007)
4. BBC News: Forged rail tickets sold on dark web, BBC investigation reveals (2016)
5. International Union of Railways: Uic 918–3: International rail ticket for home printing (2007)
6. International Union of Railways: the UIC public key management website (2017). https://railpublickey.uic.org/download.php
7. Radke, K., Boyd, C., Gonzalez Nieto, J., Brereton, M.: Ceremony analysis: strengths and weaknesses. In: Camenisch, J., Fischer-Hübner, S., Murayama, Y., Portmann, A., Rieder, C. (eds.) SEC 2011. IAICT, vol. 354, pp. 104–115. Springer, Heidelberg (2011). doi:10.1007/978-3-642-21424-0_9
8. Bella, G., Coles-Kemp, L.: Layered analysis of security ceremonies. In: Gritzalis, D., Furnell, S., Theoharidou, M. (eds.) SEC 2012. IAICT, vol. 376, pp. 273–286. Springer, Heidelberg (2012). doi:10.1007/978-3-642-30436-1_23
9. Johansen, C., Jøsang, A.: Probabilistic Modelling of Humans in Security Ceremonies. In: Garcia-Alfaro, J., Herrera-Joancomartí, J., Lupu, E., Posegga, J., Aldini, A., Martinelli, F., Suri, N. (eds.) DPM/QASA/SETOP -2014. LNCS, vol. 8872, pp. 277–292. Springer, Cham (2015). doi:10.1007/978-3-319-17016-9_18
10. Probst, C.W., Kammüller, F., Hansen, R.R.: Formal modelling and analysis of socio-technical systems. In: Probst, C.W., Hankin, C., Hansen, R.R. (eds.) Semantics, Logics, and Calculi. LNCS, vol. 9560, pp. 54–73. Springer, Cham (2016). doi:10.1007/978-3-319-27810-0_3
11. Garcia, F.D., Koning Gans, G., Muijrers, R., Rossum, P., Verdult, R., Schreur, R.W., Jacobs, B.: Dismantling MIFARE classic. In: Jajodia, S., Lopez, J. (eds.) ESORICS 2008. LNCS, vol. 5283, pp. 97–114. Springer, Heidelberg (2008). doi:10.1007/978-3-540-88313-5_7
12. Murdoch, S.J., Drimer, S., Anderson, R., Bond, M.: Chip and pin is broken. In: 2010 IEEE Symposium on Security and Privacy, pp. 433–446 (2010)
13. Schneier, B.: Flying on someone elses airplaine ticket (2003). https://www.schneier.com/crypto-gram/archives/2003/0815.html#6
14. Jaroszewski, P.: How to get good seats in the security theater? Hacking boarding passes for fun and profit. In: DEF CON 24 Hacking Conference (2016)