Secure Electronic Toll Collection

Felix Tran, Ben Wolz

Massachusetts Institute of Technology

May 20, 2021

Contents

1 Introduction

Toll roads have existed for thousands of years dating back to 7th century B.C. Intuitively, they are a way to recoup the costs of construction and maintenance of the road and eventually generate revenue from passing travellers. The concept is simple; travellers are required to pay a toll for the rights to use a road, and in the middle ages, roads even offered protection to their travellers for an additional fee. However, it was only very recently that this concept was automated using electronic tolling. U.S. Nobel Economics Prize winner William Vickrey first proposed an electronic tolling system in 1959. Dozens of companies since then have build electronic tolling ecosystems since then, the most notable being EZ Pass.

While the use of technology to automate toll transactions has eliminated many of the inconveniences associated with traditional toll roads, it has introduced many security risks as well. We begin this paper by analyzing the security of traditional electronic tolling systems and explore attacks that this system is vulnerable to. Next, we propose a more secure electronic tolling system that addresses the previously explored attacks and new attacks that the system may encounter.

1.1 Goals and Project Scope

Our goal for this project is to explore current electronic toll collection (ETC) systems' security policies, look for shortcomings in their systems, and design a new system that will address those shortcomings.

For the purposes of this paper, we will only be considering attacks that help adversaries avoid tolls. Therefore, we do not consider scenarios where an adversary attempts to block all signals between transponders and antennas. The goal of our adversary is to trick the ETC system to not charge them, not to break the system itself.

We also do not consider cases where adversaries forge license plates due to severity of charges associated with the crime[1] and the ease of being caught. Authorities can easily recognize forged license plates, and if fakes are well made, authorities can keep an eye out for the forged plate's number on any cars they see.

2 Current ETC System

Here we outline a modern ETC system. Note that not all ETC systems have these exact specifications, and some may be more or less susceptible to certain attacks.

2.1 Components

1. Transponder - Also known as a tag, the transponder is a battery-operated radio frequency identification (RFID) unit that is responsible for communicating with the toll booth's antenna. The transponder is intended to be mounted under the car's windshield for use.

2. Antenna - This is an electronic reader installed at ETC supported toll booths used to communicate with the transponder and complete toll transactions.

3. Lane Controller - This is the computer responsible for controlling the lane equipment and tracks vehicles passing through. This includes a camera that can capture license plates to be read with optical character recognition (OCR) software.

4. Central Database - All toll booth LANs are connected to a central database containing information about user accounts.

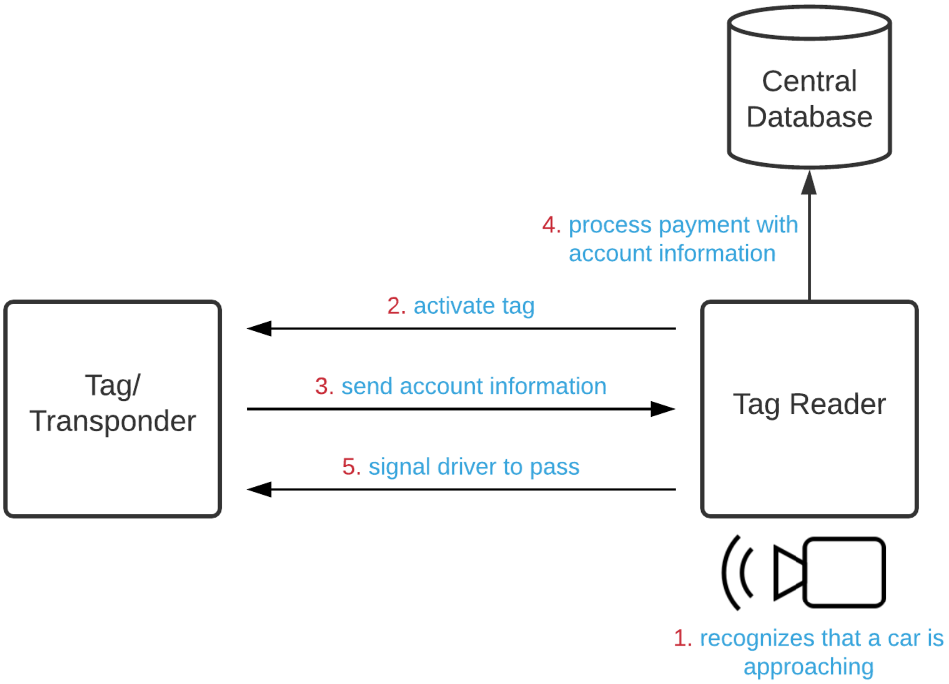
2.2 Sign-Up & Installation

To start using ETC, users establish a prepaid account using their credit card, personal check, or cash. Once the account is established, the user will receive a transponder which is an electronic chip that contains information about their account. The user should then install this transponder onto their car. After installation, each time the car goes to a toll booth that supports ETC, the transponder will share necessary information to the toll booth's antenna so that the user's account can be charged.

2.3 Tolling Protocol

As a car with a transponder approaches a toll booth supporting ETC, the toll booth's lane controller recognizes this and tells the antenna to emit a radio frequency that activates the transponder. The antenna then emits this radio frequency to activate the transponder. Upon activation, the transponder broadcasts a signal back to the antenna with account information, such as an ID. The antenna then queries the central database with this information to get the driver's account information. If the account is in good standing, the toll will be deducted from the driver's account and the driver is signaled to proceed. Otherwise, the driver can still be signaled to proceed, but the toll booth camera will record the license plate and the vehicle owner will receive a violation notice in the mail [5].

Below is a diagram of the current ETC system's protocol.


Central Database
4. process payment with account information
2. activate tag
Tag/ Transponder
3. send account information
Tag Reader
5. signal driver to pass
1. recognizes that a car is approaching

2.4 Shortcomings

Based on the scope of our adversary, these are the most common attacks that are performed against current ETC systems.

2.4.1 Physical Theft of Transponders

In this attack, adversaries physically steal a victim's transponder, replace it with a nonfunctional replica, and use the functional transponder for themselves. Once the adversary installs the functional transponder in their car, they will be able to pass ETC toll booths with their car while the victim's account is charged the toll. It can take months or even years for victims to discover that they have been victims and by then it may be too late. This is most common when users leave their car unlocked but can happen in other unexpected ways as well. In one case, a Virginia woman was involved in a devastating car accident that totaled the car. For the several months that she was focusing on recovering, someone had stolen her EZ-Pass and accumulated over $1,000$ in fraudulent charges before she noticed [2]. In another case, one stolen EZ-Pass transponder in Pennsylvania accumulated over $11,000$ in fraudulent charges before the victim found out [7].

2.4.2 RFID Skimming

In the previous attack, adversaries needed to get into a victim's car to steal the transponder. In this attack, we discuss a method that adversaries can abuse to avoid toll charges without the hassle of getting inside a victim's car. In the current protocol, an activated transponder will attempt to broadcast a signal to an antenna with a user's account information. This information is sufficient for a toll booth to charge users and allow drivers to pass. Since many toll booths do not question the information sent as long as it is sufficient, an adversary that obtains this information could potentially create a functional replica of the victim's transponder and use it for their own benefit without physically stealing a victim's transponder.

Assume Alice is a user of ETC and has a transponder in her car and Bob is an adversary. Bob can activate Alice's transponder without her knowing, record the broadcasted signal, and spoof it when he is at a toll booth. In this attack, Bob will be able to pass the toll booth assuming that Alice's account is in good standing, and Alice will be wrongfully charged the toll. On an online forum, a user commented that they would routinely find cars with EZ-Passes in a parking lot, activate the transponder, record their broadcasted signal, and spoof it to pass toll booths and avoid paying the toll themselves[3].

3 New ETC System

Here we outline our new ETC system. This system provides honest users added security without presenting major inconveniences or changes to how they interact with the current system.

3.1 Components

This new ETC system utilizes the same components for its tolling booth as the previous ETC system, the main difference is that the components may follow different protocols.

3.1.1 Hardware Components

1. Transponder - In the new system, the transponder is still a battery-operated active RFID unit. The main differences are that the transponder will be storing a specific transponder ID and the intended vehicle's license plate number and will only be emitting encrypted information.

2. Antenna - This is an electronic reader installed at ETC supported toll booths used to communicate with the transponder and complete toll transactions.

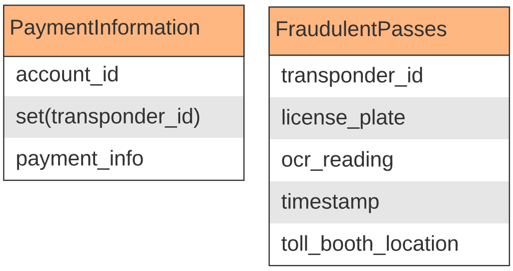
3. Lane Controller - This is the computer responsible for controlling the lane equipment and tracksvehicles passing through. This includes a camera that can capture license plates to be read withoptical character recognition (OCR) software.

   In addition to being responsible for controlling lane equipment and tracking which vehicles pass through, the Lane Controller in this system is also responsible for initiating the tolling protocol with the transponder attached to the user's vehicle. This protocol (laid out in section 3.3) requires the generation of a public key as part of an ElGamal encryption scheme, which the Lane Controller is responsible for handling for each interaction with each transponder that passes through the tolling booth.

4. Central Database - The contents of the database are different from the previous ETC system and are discussed more in (3.1.2).

3.1.2 Database Design

We make use of a relational database to store information for the tolling system. The data is arranged into the tables described in the diagram below.



PaymentInformation
account_id
set(transponder_id)
payment_info

FraudulentPasses
transponder_id
license_plate
ocr_reading
timestamp
toll_booth_location

The data is arranged in this manner to efficiently handle the use cases described later in the paper. When an honest user passes through the tolling station, a single query can be made to the PaymentInformation table to effectively deduct the necessary amount from their balance. For passes where it is suspected that an adversary may be using another driver's transponder or in the event of equipment failure, the vehicle's license plate will be billed, and the FraudulentPasses table is used to document the pass where an adversary may be suspected so users and authority can be made aware of the event.

3.2 Sign-Up & Installation

3.2.1 User

To start using this new ETC system, users establish a prepaid account using their credit card, personal check, or cash just like before. The only difference for the user now is that once the account is established, users must provide the license plate numbers of the cars they intend to have transponders for in order to receive their transponders.

3.2.2 ETC Provider

The reason that users must provide the license plate numbers of the cars they intend to use is because of the new protocol that the new ETC system uses. In order to avoid adversaries from simply tampering with a user's transponder and replacing the stored license plate number with their own, transponder's will be storing a transponder ID, T, and a license plate number, LP, such that

$$\text{SHA256}(T||LP) < V$$

Where V is a security parameter chosen by the ETC company. This requires the ETC company to do some work in order to find a valid transponder ID T for the transponder. Once this T value is found, it is stored under the user's account information so that T can be used to retrieve the user's account during tolling transactions. V can be adjusted to increase or decrease the difficulty of finding this T value which will in turn make it easier or harder for adversaries to successfully tamper with a user's transponder. More information on this can be found in (3.4.3).

3.3 Tolling Protocol

The new tolling protocol used to handle a tolling event in the new ETC System involves the transponder and antenna using the ElGamal encryption scheme.

- $\text{Gen}(1^k) \rightarrow (PK, SK)$
  1. Select a **safe prime** $p \in \{0,1\}^k$
  2. Choose a random $x \leftarrow \mathcal{Z}_p^*$ and let $g = x^2 \bmod p$
  3. Choose a random $s \leftarrow \mathcal{Z}_q$ s.t. $q = \frac{p-1}{2}$
  4. Output $(PK, SK) = ((p, g, g^s), (p, g, s))$
- $\text{Enc}(PK, m)$
  1. Choose a random $r \leftarrow \mathcal{Z}_q$
  2. Output $(g^r, g^{sr} \cdot m)$
- $\text{Dec}(SK, c)$
  1. Output $m = \frac{c}{(g^r)^s}$

The above is provided as a reference for the Tolling Protocol defined below. To keep the scheme concise, variable definitions have been left out of the individual steps, however they all follow the definitions laid out above. Please use the general scheme as a reference point for variables in the tolling protocol.

1. As the car approaches the toll booth, the lane controller
   (a) recognizes that the car is approaching

   (b) reads the approaching car's license plate, LP_{ocr}

   (c) calls Gen$(1^k) \rightarrow (PK, SK)$

2. Next, the lane antenna emits a radio frequency to activate the tag/transponder and communicate PK to the tag/transponder inside the approaching car.

3. The tag/transponder inside the car then

   (a) calls Enc(PK, m) where $m = T||LP_t$[1]

   (b) sends the output of Enc(PK, m) to the toll booth's antenna

4. The antenna then

   (a) calls Dec$(SK, g^{sr} \cdot m)$

   (b) verifies that SHA256$(m) < V$

   (c) isolates T and LP_t

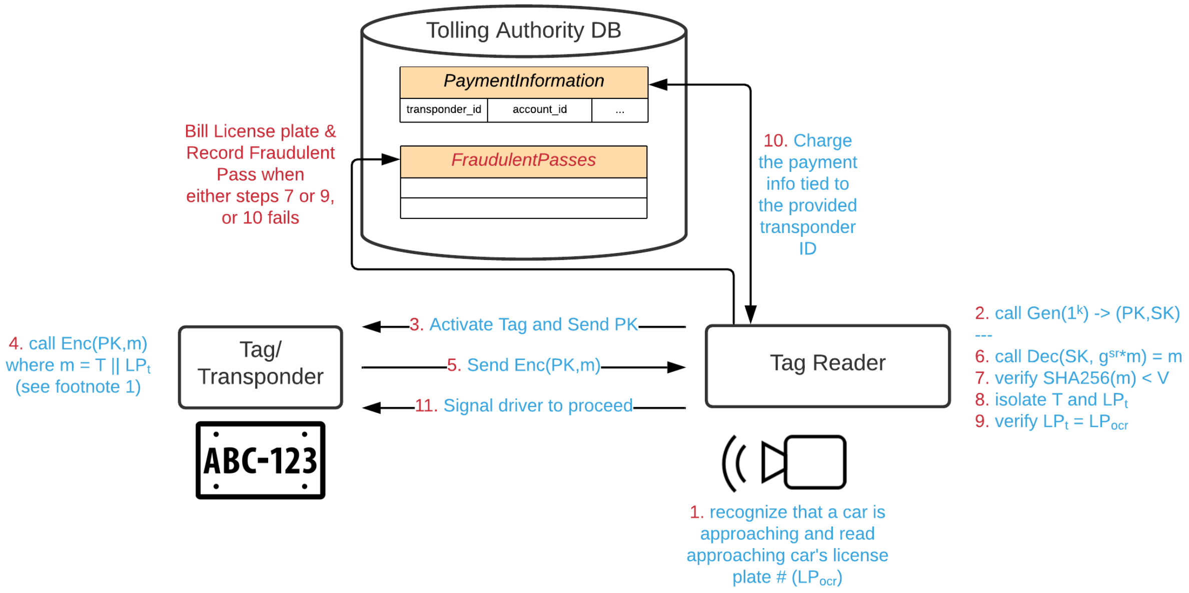
   (d) verifies that $LP_t = LP_{ocr}$

   (e) uses T to query the PaymentInformation database for the user's account and charge the toll

   (f) signals the driver to pass

If steps (4.b), (4.d), or (4.e) fail, the event will be logged in the FraudulentPasses table and users may still be signalled to pass, but the vehicle owner will receive a violation notice in the mail which is tracked via the car's recorded license plate LP_{ocr}.

Below is a diagram of the new ETC system's protocol.


Tolling Authority DB
PaymentInformation
transponder_id
account_id
...
FraudulentPasses
Bill License plate & Record Fraudulent Pass when either steps 7 or 9, or 10 fails
10. Charge the payment info tied to the provided transponder ID
2. call Gen(1^k) -> (PK,SK)
---
6. call Dec(SK, g^{sr}*m) = m
7. verify SHA256(m) < V
8. isolate T and LP_t
9. verify LP_t = LP_{ocr}
4. call Enc(PK,m) where m = T || LP_t (see footnote 1)
Tag/ Transponder
3. Activate Tag and Send PK
5. Send Enc(PK,m)
11. Signal driver to proceed
Tag Reader
ABC-123
1. recognize that a car is approaching and read approaching car's license plate # (LP_{ocr})

3.4 Security Guarantees

As noted in section (1.1), we are only concerned with attacks that help adversaries trick the system to avoid tolls. There are several methods an adversary can attempt to pass through a toll booth without incurring any fees, but the proposed system utilizes OCR to ensure that neither the adversary gets away without repercussion nor do any honest parties incur cost because of the adversary's actions.

[1] T is a transponder ID and LP_t is the license plate number stored in the transponder.

3.4.1 Physical Theft of Transponders

In this attack, much like with the original system, a malicious party physically breaks into a transponder owner's vehicle and steals the transponder. From this point, the thief could install the transponder into their own vehicle and attempt to use it at a toll booth. When the thief arrives at the booth, the tolling protocol will initiate and the driver will go through the tolling station, but the owner of the transponder will not face a charge. Based on the Tolling Protocol, the malicious party will be immediately caught for fraud thanks to step (4.d) in the protocol which compares the license plate provided by the transponder with the physical plate on the vehicle that is registered by the OCR. In this case, the system will know not to proceed with the transaction using the transponder ID but rather charge using the license plate on file.

If an attacker were to replace their own license plates with copies of the original transponder owner's (or make use of temporary tags [6] that can't be traced back to the driver), the Tolling Protocol described in this paper will not be effective in preventing the fraud. However, as this offense is considered a Felony in many states[1], we do not consider this active of an adversary within the scope of this system. Further measures could be taken through enhanced OCR technology that could detect vehicle make and model information to make this sort of fraud harder.

3.4.2 Spoofing Account Information via RFID Skimming

One way the ElGamal encryption scheme proposed in section 3.3 could be abused is if the encrypted message m was easily discoverable by a passive adversary who could then use it to steal the shared key. For example, if the account ID and license plate were encrypted separately with the same shared key as such (adapted from step (2.b) of the Tolling Protocol):

$$Enc(PK, m) = (g^r, g^{sr} \cdot license\_plate, g^{sr} \cdot account\_id)$$

An adversary who knew the license plate associated with a given transponder (which can be detected through simple visual inspection) could easily discover the shared key by dividing the value of the license plate from the first ciphertext and using that to then discover the transmitted account information in the second ciphertext.

This form of attack is prevented by the Tolling Protocol thanks to the encryption construction, where the message to be encrypted is actually a concatenation of the account ID and license plate. A skimming adversary cannot actually leverage the known license plate value to reveal any information about the shared key. Suppose a passive adversary listening in on the correspondence between a transponder and a toll booth was able to skim $c = (g^r, g^{sr} \cdot m)$. One concern with the proposed Tolling Protocol is that because the transponder owner's license plate is effectively publicly available, a passive adversary could learn the transponder owner's license plate, skim the value of c from the toll booth antenna, and then divide out the value of the license plate to get the shared key. From here, the adversary could use the shared key to decrypt the driver's account information, which could be then used in a spoofed transponder with another to simulate another vehicle that would pass OCR inspection with a different account ID.

Additionally, the protocol prevents passive adversaries from simply reusing the entire skimmed ciphertext because in each interaction with a toll booth the booth and the transponder both provide new, indistinguishable from random public keys. This means the third step in the encryption would produce an invalid decryption that could not be used to identify a billable account ID or license plate number.

3.4.3 Theft and Tamper

We now highlight the security guarantee that is provided by the hash generated by

$$\text{SHA256}(T||LP)$$

defined in section (3.2.2). Suppose that an adversary were to physically steal a users transponder. As explained in (3.4.1), this transponder alone will not be enough for an adversary to drive through a booth toll-free because the toll station's OCR will read a different license plate number than what comes up on the transponder. If an adversary wanted to use a stolen transponder, they would have to modify the transmitted license plate to match their own. However, we argue that the work required to find a valid transponder ID drastically outweighs the cost of being an honest participant in the system.
For an adversary to successfully use a stolen transponder, they must first do two things:

1. Modify the transponder's transmitted license plate number to match their vehicle's license plate number
2. Modify the provided transponder ID such that, for the modified T^*:
   (a) $\text{SHA}(T^* \| LP) < \text{V}$
   (b) T^* is a transponder ID that is recognized in the ETC provider's database

First, the adversary is constrained by the amount of work required to compute a given T^* that satisfies the hashing constraint. Additionally, the adversary must pick a transponder ID that exists for another user, which, without direct access to the database, requires trial and error. That is, an adversary could satisfy the hashing constraint but has no way to guarantee they've selected an ID that corresponds to a transponder. Given these two constraints, we argue the work required to successfully hack a transponder would likely outweigh the cost of simply being an honest participant.

3.4.4 ETC Response to Suspicious Passes

In the event that a tolling station handles a pass where the license plate read by the OCR and the license plate transmitted by the transponder do not match, it is assumed that either the OCR failed to read the license plate properly or the vehicle is being used by a party who stole the transponder.

If the OCR reading does not match the license plate in the database, the event is deemed a fraudulent pass, and is recorded in the database. Since each transponder ID is tied to a user account, a user can have access to all fraudulent events that take place using one of their owned transponders. While we do not discuss the UI further in this paper, it is suggested that the tolling authority provide a list of all fraudulent passes associated with a given user so they can be aware of any issues tied to their account.

3.5 Physical Considerations for ETC Stations

To ensure that this system can fully scale to a multi-lane highway with multiple tolling stations, we propose the following to ensure the construction of the tolling station does not interfere with the stated protocol. First, each tolling station should have an individual tag reader for communicating with a given vehicle that passes under it. This will prevent neighboring tolling stations from unintentionally transmitting data from their interactions to the wrong station and inadvertently causing a fraudulent read. Additionally, to mitigate any possible inaccuracies that could come from the OCR device, consider building awnings above the toll stations so that inclement weather such as snow or rain does not impact the accuracy of the OCR reading. In any case, if an OCR reading fails, the database will still be queried on a user's transponder ID, however it would mitigate risk and additional queries to ensure OCR accuracy.

4 Related Works

In this section we briefly discuss two related ETC system designs. While each of these designs poses their own strengths, we contend that they are not necessarily optimized for the same use case as the system presented in this paper.

4.1 OCR-Based ETC

The use of OCR raises the question of why not build a system that only uses OCR for validation. In this system, a given transponder would emit an ID which is then referenced in the database to ensure the license plate scanned by the OCR is valid. This system could cover the same guarantees the presented system covers, however this system is not optimized for the same level of performance. Consider the fact that in the proposed system today, an honest user will only require the toll station to send a single query to the database to charge the account. If we consider this to be a deduction of a given toll amount, we can see that the tolling station does not have to wait for a response from the database before finishing the protocol. In the case of an OCR-Based system, the tolling station would have to execute a DB query and wait for the response to come back before validating the ride. Thanks to the local check made by our protocol, the tolling station need not make any queries that it must wait for a response for.

It is clear there is a trade-off of complexity here. The OCR-only system provides a much simpler and more intuitive protocol, however it guarantees a database query that the system must wait for for every pass. Scaling this up to the millions of passes vehicles make through tolling stations, these queries add up to a substantial amount of time and energy that our system can avoid while still guaranteeing security.

4.2 GPS-Based Tolling Systems

A novel form of ETC systems have been proposed that use GPS tracking of user vehicles to record vehicle movements in a privacy preserving method with a pay-as-you-go pricing model[4]. This system is beneficial in urban areas where certain drivers are travelling in high-congestion inner city roads because it appropriately charges drivers that make use of the roads the most. However, this system has shortcomings in terms of its current network effects regarding actual use as well as a lack of existing infrastructure. Therefore, while this system does prove to be promising for future ETC systems, the current infrastructure would be more positively impacted by security overlaid on top of the existing infrastructure.

5 Conclusion

In this paper, we present a secure electronic tolling system as a response to the shortcomings of current ETC systems. The secure electronic tolling system combines cryptographic protocols with existing tolling technologies including OCR to ensure users that theft of their ETC transponders, whether by physical theft or means such as RFID skimming, will not enable adversaries to impersonate as the driver when passing through a tolling booth. The central focus of the secure electronic tolling system is to prevent attacks whereby adversaries can avoid paying tolls at the expense of other users, and the design of the system we propose achieves that.

References

[1] New york license plate offenses. *https://www.tilemlawfirm.com/new-york-license-plate-offenses.html.*

[2] Virginia woman on the hook for $1,000 billed to e-zpass stolen after severe car wreck. *https://www.nbcwashington.com/news/local/virginia-woman-on-the-hook-for-1000-billed-to-e-zpass-stolen-after-severe-car-wreck/69821/.*

[3] How secure is e-z pass? *https://security.stackexchange.com/questions/174369/how-secure-is-e-z-pass*, November 2017.

[4] R. Blumberg, A. & Chase. Congestion pricing that respects driver privacy. *ITSC*, 2005.

[5] K. Bonsor. How e-zpass works. *https://auto.howstuffworks.com/e-zpass.htm*, February 2021.

[6] Texas Transportation Institute. Study of systems for issuing temporary tags for unregistered motor vehicles in texas. October 2006.

[7] R. Longley. Beware these dangerous e-z pass scams. *https://www.thoughtco.com/dangerous-ez-pass-email-scam-3321160.*