GIAC
CERTIFICATIONS

Global Information Assurance Certification Paper

Copyright SANS Institute
Author Retains Full Rights

This paper is taken from the GIAC directory of certified professionals. Reposting is not permited without express written permission.

Interested in learning more?

Check out the list of upcoming events offering
"Security Essentials (Security 401)"
at http://www.giac.org/registration/gsec

Electronic Toll Collection

An Introduction and Brief Look at Potential Vulnerabilities

© SANS Institute 2004, Author retains full rights.

Name: Don Flint
Submitted: April 27, 2004
Certification: GSEC
Version: 1.4b
Option: 1

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

Table of Contents

Table of Contents i
Abstract ii
Introduction 1
Electronic Toll Collection Overview 1
Automatic Vehicle Classification (AVC) 2
Automatic Vehicle Identification (AVI) 3
Violation Enforcement (VE) 3
Vulnerable Points and Exploitation 3
Nonpayment 4
Jamming 4
Eavesdropping 5
Collection 5
Build Your Own Token 6
Infrastructure Vulnerabilities 6
Backbone Connectivity 6
The Databases 7
Other Information Stores 7
Summary 7
References: 9

© SANS Institute 2004, Author retains full rights.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

Abstract

Since 1992 active Radio Frequency Identification (RFID) tags have been used in vehicles to automate the toll process on toll roads, bridges, and tunnels in a process called Electronic Toll Collection (ETC). These tags are mounted to the windshield or externally surrounding the license plate on a vehicle and read as the vehicle proceeds without stopping through special lanes at the toll plaza. This paper looks at the security behind these transactions and the possibility for this toll process to be compromised. It also addresses the supporting infrastructure briefly as a standard banking network. Given the state of the art within the automated toll collection process and systems, it is indeed possible to cheat this system through a variety of means on a small scale. However all of the methods to cheat have inherent in them significant risk of identification and thus prosecution. The backend infrastructure should be further examined for large-scale disruption potential.

© SANS Institute 2004, Author retains full rights.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

Introduction

One of the biggest complaints of motorists using toll roads is the congestion and delay caused by stopping to pay at the tollbooths. Many toll authorities have searched for ways to improve the toll collection process. Over the last decade, a significant improvement in this process was implemented and dubbed Electronic Toll Collection (ETC). As these ETC systems are gaining widespread use throughout the country and even the world, efforts are being made to improve and expand their interoperability similar to the way home bulletin board systems (BBS) grew first into local networks and finally into Internet Service Providers (ISPs). There may come a day in the not to distant future where automobiles have built-in transponders that can be registered with the local toll authority yet used throughout the country for toll roads and parking.

On the east coast of the United States, the E-Z Pass ETC system (also called EZPass, EZ Pass, EZ-Pass and even Easy Pass) is an example of an interoperable ETC system which appears to be the forerunner of an ETC system spanning the entire continent. It includes the New York State Thruway Authority and the New York Bridge Authority in New York, The Port Authority of NY and NJ, the Massachusetts Transportation Authority Bridges and Tunnels, Delaware Department of Transportation (DelDOT), and taking in such smaller systems as the SmartTAG in Virginia and the M-Tag system in Maryland. A listing of the current participating toll systems can be found on the E-Z Pass website[1]. E-Z Pass ETC will be used as the primary example system for the remainder of this paper.

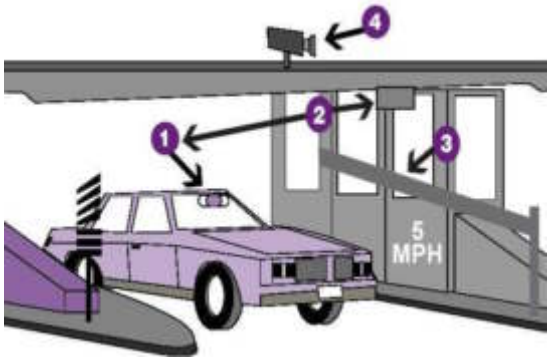
Electronic Toll Collection Overview

The following figure from "Your Guide to E-ZPass" shows the basic toll plaza configuration for an ETC system.

[1] http://www.ezpass.com/static/info/facilities.shtml

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

Figure 1: How the E-ZPass System Works[2]



1. As you slowly pass through the E-ZPass facility, your *E-ZPass tag* is read.
2. In an instant, the tag information is read by an *overhead antenna* in the E-ZPass facility and the proper charge is deducted from your E-ZPass account.
3. At some facilities, there are *gates* that will go up when a valid tag is read.
4. A *video enforcement system* is in place to identify charge evaders.

The toll plaza equipment consists of a lane controller, toll violation cameras, treadles, variable message signs (VMS), detector loops, and lane transponders. The lane controller coordinates all of the information from each transaction and interacts with the Plaza Local Area Network (LAN). The Plaza LAN connects either via wide area network (WAN) or direct connection to the appropriate service center for the toll road in question.

Each of the participating E-Z Pass toll authorities maintain their own service centers that issue the transponders and maintain the accounts for their local patrons. The centers receive and correlate all of the transactions from the toll plazas it services and adjusts the accounts of the patron, then sending the transaction result back to the plaza within milliseconds. These centers interact when patrons from one center use the toll services of another center.

ETC is generally broken up into three pieces; automatic vehicle classification (AVC), automatic vehicle identification (AVI), and violation enforcement (VE).

Automatic Vehicle Classification (AVC)

Classification of the vehicle is extremely important for those plazas where the fare is dependant on the number of axles on the vehicle, a very common case throughout the E-Z Pass ETC. Sensors, called treadles, are embedded in the roadway to count the axles and determine the tire width. Additional sensors similar to the motion sensors found on automated doors detect the presence of the vehicle and help distinguish and individualize the vehicles. Such sensors use the latest technologies magnetic induction loops, treadles, and laser imaging.

[2] http://www.ezpass.com/static/downloads/i_guide.pdf "Your Guide to E-ZPass" 11/02

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

Automatic Vehicle Identification (AVI)



The AVI component of the system consists of the RFID transponder such as the one seen to the right[3] is located in the automobile and the equipment to communicate with the transponder located at the toll plaza and the License Plate Recognition (LPR) subsystem, a good primer of which can be found at License Plate Recognition - A Tutorial[4]. While the toll plaza RFID transponder equipment is generally called a reader, in most ETC systems it can also write information to the vehicle transponder such as the time, date, location and vehicle class of the transaction.

Violation Enforcement (VE)

Violation enforcement consists of using the identification elements gathered from the AVC and AVI components along with additional information such as license plate and vehicle images to allow authorities to collect from and/or prosecute those who violate the electronic toll plaza. Typical ETC violations are:

- Use of electronic toll collection lanes without a vehicle transponder,
- Insufficient funds in the associated account for identified transponders,
- Use of a transponder from a low-toll vehicle such as a car with two axles in a high-toll vehicle such as a tractor trailer.

Vulnerable Points and Exploitation

In The Art of War[5], Sun Tzu laid out the maxim that it is important to know your opponent in order to beat them. That maxim applies as much in the cyber world as elsewhere. For someone to take advantage of weaknesses within the system, those weaknesses must be known. There are two main types of vulnerability points for the ETC systems. The first type of vulnerability is to the backbone infrastructure, a traditional network security puzzle unique only in the end elements that make it up. The second type of vulnerabilities is at the toll plaza during a transaction.

Focusing on the latter vulnerability first shows that in truth, some of the weaknesses are taken advantage of unwittingly every day but are counted as luck or chance on the part of the recipient. Since the reader system is not perfect

---

[3] http://www.state.nh.us/dot/graphics/ezpassmodule.jpg from http://www.state.nh.us/dot/turnpikes/ezpass.htm, the New Hampshire Department of Transportation website announcing the new E-Z Pass installation.

[4] http://www.licenseplaterecognition.com/ License Plate Recognition - A Tutorial

[5] http://www.chinapage.com/sunzi-e.html "SUN TZU ON THE ART OF WAR THE OLDEST MILITARY TREATISE IN THE WORLD" Chapter 3, Verse 18.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

but runs at accuracy in the 98% to 99%[6] range, many people each day pass by the tolls either without being charged at all, or by being wrongly charged. It is up to the consumer to complain when s/he has been wrongly overcharged, but the system does not know to whom the charge should be redirected so it is thrown out. The transponders are generally only good for a year or two before the embedded battery needs replacing.

Counting on being in the inaccurate range and not on the overcharged side would not really be considered exploiting the system. The patron has little control over these items. However, the patron can influence the transaction process in multiple ways. The influence is only for the single transaction and does not affect the other patrons sharing the toll facility.

Nonpayment

One of the most obvious points at which to fool the system is during the collection phase. It is the equivalent of dropping the dime in the basket of mechanical toll systems or handing the cash over to that smiling and friendly tollbooth operator. Fooling the system is easy. Getting away with it isn't. The easiest way to fool it is simply to drive through the electronic collection lane without a transponder. This will be immediately recognized by the system, however most of the toll plazas have no mechanism for stopping the offender, in fact they want traffic to keep flowing and state specifically that should the red light indicate non-toll collection, the driver should keep going to avoid delays and/or accidents. The system operators would like you to call them and provide payment for the missed tolls. They can try to get your vehicle information from the appropriate Department of Motor Vehicles and then either send you a bill on their own or forward the information of the non-payment to law-enforcement for prosecution. However, since the payback is so small and the costs to recover so large, the authorities seem to tolerate some slippage in the system, especially given that the system is not 100% accurate. Just remember that the modern toll plaza does have those wonderful cameras taking pictures of the license plates and, in some cases, of the drivers.

Jamming

Ok, so most of the time you want to be able to appear to be a legitimate user. Your daily commute is improved by use of the faster toll lanes. In another state on vacation you decide to avoid both the hefty tolls and the tracking of your movements so you pop your transponder off the window and drop it in the convenient "read prevention" bag supplied by Customer Service or purchased from one of the other available online sources such as the mCloak from mobileCloak[7] and race through the electronic toll collection lane. Whoops. As a

[6] http://www.nbc6.net/print/1419822/detail.html

[7] http://startsimple.com/mobilecloak/index.html

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

registered user of the system, your license tag is known to the system and the system operators don't have to query DOT to find out who you are or where you live. Once they figure out which car went through based on the AVI subsystem, they don't have to send it to collections, they will just deduct it from your account and send you a notice that your tag is not working. Still, all is not lost. At this point you can wait to see if they call and ask for their money or if they just tack it on to your bill. Still, without the reader the identification is less accurate though made much better due to improvements in the hardware and software for LPR in recent years.

Eavesdropping

Is the system subject to eavesdropping and replay attacks? Is it possible to sit on the side of the road near a toll plaza, perhaps with some feigned automotive problem, and collect the transaction? It would take some pretty intensive equipment but it is possible. With the signal, you can try to either replay it directly, or decode it and grab out just the responses to replay. Some of the difficulties in this technique are:

- Encoded Signals: the signals are encoded using the Manchester Encoding scheme[8]. While the Manchester encoding is not encryption, it does require implementing the correct decoding algorithm to obtain the original signal.
- Directional Antennas/Weak Signals: the antennas on both the auto and in the toll lane are highly directional, not only for security but to reduce cross-talk between toll lanes.

Once the signals have been collected and processed, there is still the difficulty of replaying the signals or creating a new RFID token with the stolen information (see Build Your Own Token below). Analysis of the signal itself is beyond the scope of this introductions but could provide an interesting follow-up research topic.

Collection

With all of those cars in the parking lot with their tags so prominently displayed in the window it is tempting to consider borrowing one of them to provide legitimate identification. The truly devious would steal two tags, putting the first in the place of the second so the auto owner doesn't report a stolen tag, then using the second one. Switching tags every few days would leave a confusing trail for law enforcement to unravel. On the down side once again are the cameras and other components of the AVI and VE systems designed to identify such tag uses, even after the fact. On the up side, by switching tags, the AVI system will also tag those innocents as wrongdoers and provide for plausible deniability. This technique suffers from the repeated breaking into automobiles to switch tokens, each even increasing the risk of being caught and with much greater

[8] http://homepage.ntlworld.com/matthew.rowe/micros/virbook/manchest.htm

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

consequences than simple toll evasion.

Build Your Own Token

The easiest way to build your own token is if you have physical access to the ETC transponder and a transponder tag programmer such as those offered by Sirit Technologies[9]. In addition to the detailed information about the system and programming of the tokens, one crucial piece of information would be required, the transponder ID. This can be obtained in one of three ways:

- Eavesdropping at a toll plaza,
- Make one up,
- Copy one from another transponder.

As with most other certificate-based systems, without the server having the information about the client, it doesn't do any good to put a fake certificate out there. It will just read as an error and raise a flag in the system. On the other hand, it could be seen as a normal system error and ignored. Still, the cameras looking at the license plates will probably eventually be checked to see if it is a valid user.

Infrastructure Vulnerabilities

Instead of trying to thwart the collection process directly, someone could look at the infrastructure that supports the ETC system. From the viewpoint of malicious intent greater in scale than simple toll fraud, the infrastructure is where it would make the most sense to concentrate efforts. According to a prepublication copy of a report, "Cybersecurity of Freight Information Systems,"[10] the trucking system carries over $7 trillion and nearly 11 billion tons of cargo annually. On the east coast, many of the trucks carrying this cargo are equipped with E-Z Pass transceivers. A wide-scale shutdown of the E-Z Pass ETC would cause massive delays and disruption to that freight system. Fortunately, the E-Z Pass system is decentralized making it more difficult to affect multiple centers. Unfortunately, it also means there are more ingress points that need to be secured.

Backbone Connectivity

The backbone network for the E-Z Pass systems are, for the most part, sonnet fiber optic networks run from the toll plazas back to the customer service centers. Connection between the service centers utilizes the same types of networks found throughout the rest of cyberspace; leased lines, VPNs, and private networks. The details of this connectivity is not publicly available over the Internet but would a good topic for follow-up research.

---

[9] http://www.sirit.com/default.asp?sectionID=4&action=open&pageID=25

[10] http://www.securitymanagement.com/library/Freight_cybersecurity1003.pdf

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

The Databases

All of the patron information is stored in various databases at the customer service centers servicing a particular toll segment. Due to the information contained in these databases, they are required to be protected under various privacy acts. Coordination between these databases is constant as patrons transit the entire E-Z Pass network. These databases are the true crown jewels in the ETC systems and should be the most protected. Compromise of these databases could yield anything from a single patron being able to avoid tolls to complete shutdown of the entire ETC system.

Information about the specifics of these databases was not publicly available over the Internet despite numerous searches. This information would need to be obtained either from an insider or by compromise of the external protections or possibly by careful search through and analysis of public reports from the toll authorities. Unfortunately such search is beyond the scope of this introduction but would be a good topic for follow-up research.

Other Information Stores

The E-Z Pass system provides email notification to users who register for such service. The email portion of the system was hacked into in late 2000 by Christopher Reagoso[11] to demonstrate a system vulnerability[12]. The information on the account was put in a static web page without authentication and the URL emailed to patrons. By replacing the account number in the URL with another, Reagoso was able to view the usage information of other patrons, but not able to directly access the backend datastore about that patron such as address and credit card information. Needless to say that particular hole was patched very quickly.

While the account usage hole discovered by Reagoso was certainly an embarrassment to the E-Z Pass system, it was not a vulnerability that could be directly exploited to shut down the system. Further, it did not provide access to the back-end databases which are of primary importance. It was, however, an indication that security is not the primary driver in the development and maintenance of the E-Z Pass data resources.

Summary

While it is quite easy to circumvent the security at the toll plaza for the new RFID based electronic toll collection systems, it is not easy to continue to get away with it. These transactions are quite small in scale and do not offer the possibility of mass disruption.

---

[11] http://archive.infoworld.com/articles/hn/xml/00/10/25/001025hnezpass.xml InfoWorld, October 25, 2000.

[12] http://md.hudora.de/blog/guids/17/72/0001024000001577.html

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

The back-end networks appear to be as secure as most other online transactions and perhaps even a bit more so since they are being treated as banking applications. Detailed information about the structure and composition of these networks and their interconnections and protections are not publicly available. While many website abound to provide consumer information about the E-Z Pass system, none of them seem to be run by the companies hired to actually run the infrastructure. Further research into the infrastructure security is where effort still needs to be concentrated to ensure the ETC link in the transportation system does not become the weak link enabling terrorist or other cyber warriors a viable target.

© SANS Institute 2004, Author retains full rights.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

References:

1. Vollmer Associates, LLP "E-Z Pass Evaluation Report." August 2000. URL: http://www.itsdocs.fhwa.dot.gov/jpodocs/repts_te/@6L01!.pdf
2. Dornseif, Maximillian. "EZ-Pass discovers risk of sending URLs instead of actual text." October 2000. URL: http://md.hudora.de/blog/guids/17/72/0001024000001577.html
3. Grygo, Eugene. "New Jersey Turnpike electronic toll collection system hacked." October 2000. Infoworld url http://archive.infoworld.com/articles/hn/xml/00/10/25/001025hnezpass.xml
4. Sirit Technologies. "Electronic Toll & Traffic Management, Tag Programmers." 2003. URL: http://www.sirit.com/default.asp?sectionID=4&action=open&pageID=25
5. Dattalo, Scott "Manchester encoding explained." URL: http://homepage.ntlworld.com/matthew.rowe/micros/virbook/manchest.htm (March 2004)
6. NBC 6. "SunPass Glitches Cause Concern, NBC 6 Investigative Report: Overcharged By SunPass." 2002 URL: http://www.nbc6.net/print/1419822/detail.html
7. Pei, Ming L. "SUN TZU ON THE ART OF WAR, THE OLDEST MILITARY TREATISE IN THE WORLD." 1995-2004 URL: http://www.chinapage.com/sunzi-e.html Translated from the Chinese By LIONEL GILES, M.A. (1910)
8. New Jersey E-Z Pass Customer Service Center. "E-Z Pass Customer Reference Guide." URL: http://www.ezpass.com/static/downloads/i_guide.pdf
9. New Hampshire Department of Transportation. "New Toll Collection System and E-ZPass Implementation Project Status Update..." URL: http://www.state.nh.us/dot/turnpikes/ezpass.htm
10. Hi-Tech Solutions, Hofman, Yoram. "License Plate Recognition - A Tutorial." May 2003. URL: http://www.licenseplaterecognition.com/
11. New Jersey E-Z Pass Customer Service Center. "Summary of Facilities Accepting E-ZPass." URL: http://www.ezpass.com/static/info/facilities.shtml
12. Wilson & Company, Inc. "C-470 Corridor, Glossary of Definitions." October 2003. URL: http://www.c470.info/glossdefs.html
13. National Research Council of the National Academies. "Cybersecurity of Freight Information Systems, A Scoping Study." 2003. URL: http://www.securitymanagement.com/library/Freight_cybersecurity1003.pdf United States, ISBN 0-309-08555-1

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.