A Survey of Security in Single-Purpose Systems

Every time [some software engineer] says, "Nobody will go to the trouble of doing that," there's some kid in Finland who will go to the trouble. – Alex Mayfield (The Art of Intrusion, Kevin Mitnick.)

Moshe Katz, Yehuda Katz
spssrg@umd.edu

Abstract

This paper provides a security analysis of several systems used for financial transactions, security and building automation that are commonly used around the University of Maryland and by the greater public. These systems all have various security vulnerabilities, ranging in severity from causing an annoyance to completely defeating the purpose of the system. The consequences can be as small as 10 minutes of wasted class time or a dollar stolen, or the theft of thousands of dollars from a protected area without any evidence. More than attacking any particular system, this paper will present the general types of attacks that we found to be possible on a variety of consumer-grade systems. Because most companies are reluctant to even talk about security problems, we did not carry out our attacks on their live systems, but we did our best to simulate those attacks.

Table of Contents

Acknowledgements

We would like to thank all the professors who helped and encouraged us to complete this study. We would especially like to thank all the people and companies that allowed us to use their systems to test our hypotheses and discoveries. Special thanks to the regular system users who put up with the crazy things we did that got in the way of their regular work. Several of our leads came from professional installers, system maintainers and researchers who did not realize the value of the information they provided. For their protection, we will not reveal their identities. There are also several people who we would like to thank by name, but who have unfortunately asked us not to do so. To all of them we say, Thank you.

We would like to thank the state agencies and private toll roads that put up with our carefully crafted requests for information and actually once in a while answered them.

Thank you to Dr. James Purtilo for always being interested in what we wanted to discuss with him (or for at least seeming to be). We would also like to thank Dr. Purtilo for pushing us to see the connections between all the systems we researched, whether they made it into this paper or not.

Thank you to Dr. Elaine Shi for agreeing to be our advisor at the last minute, including sponsoring our CMSC390 course, and providing great resources to help us finish this paper.

Thank you to Dr. William Gasarch for always giving us great advice and for putting up with our administrative difficulties and actually sponsoring our CMSC390 course, for which this paper is our final deliverable.

Bibliographical Note: The majority of information contained in this paper comes from the authors' personal experiences based on experimentation and interaction with the systems that we investigated. Technical details about the Lenel system come from a past University of Maryland Computer Science departmental honors report, Magnetic Swipe Card System Security (Daniel Ramsbrock, Stepan Moskovchenko, and Christopher Conroy, 2008). These pieces of information are not individually cited to prevent a cluttered and broken flow of text.

Note Regarding Redacted Information: At the recommendation of University of Maryland and outside legal counsel, we have redacted certain sensitive pieces of information. We apologize for the broken flow of text in these sections.

Introduction

While cyber-security has become the new overused buzzword for marketing departments everywhere, companies should not discount the security profile of their applications, especially when those applications are high-profile public services whose misuse has the ability to impact a large number of people. We will look at the security measures in a variety of embedded systems, including contactless payment and industrial control systems.

E-ZPass is an electronic toll-collection system used across the eastern United States. Vehicles using the system are equipped with high-power RFID tags that are read by readers on the toll gantry. While E-ZPass retrofitted toll plazas require the vehicle to slow down while transiting, modern E-ZPass Express gantries allow the vehicle to maintain speed while passing through the toll. In addition, E-ZPass can be used to pay for parking in some airport parking lots. We will look at the protections in place in the E-ZPass system to ensure the integrity of the RFID transactions and prevent tag-spoofing.

Crestron industrial control systems are used for many tasks and they can be found in most general-purpose classrooms at this University. These systems control the classroom projectors and, in some classrooms, the lights. Many of those systems are connected to the campus network to allow control from the instructor's computer. We will demonstrate how these systems are vulnerable to an attack from the internet and explain what should be done to secure these systems.

Digital Security Controls (DSC) is one of the largest manufacturers of alarm and access control systems in North America. While these systems are generally connected to a central monitoring company by telephone, increasingly these systems use the internet as their primary means of communication. We will demonstrate how these systems are vulnerable to an attack from the internet and explain what should be done to secure these systems.

Secure Security Systems

Because this study was inspired by a study about the security of the Lenel OnGuard access control system used at the University of Maryland, it is fitting that we start by looking at a security and access control system. DSC is a subsidiary of Tyco International, one of the largest competitors of United Technologies, the maker of the Lenel OnGuard system. The DSC brand includes home and commercial security and fire alarm systems and building access control systems.

System Information

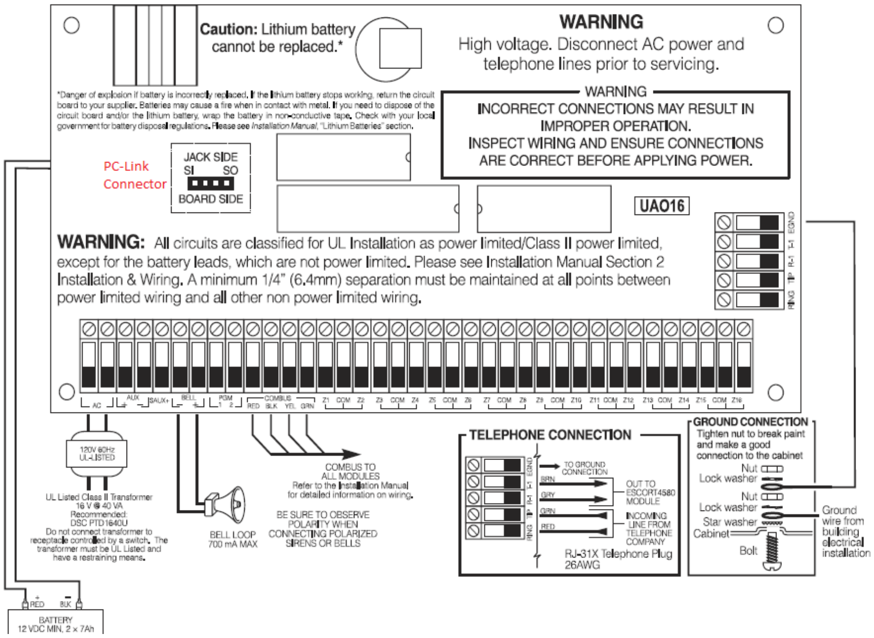
A commercial alarm and access control system is built with one primary alarm panel[1] which communicates with keypads, door controllers[2] and other peripherals over a four wire serial bus.[3]

[1] We used the DSC PC4020, a 16-zone basic alarm system.

[2] We used three of the DSC PC4820 to control 5 doors.

[3] Called the COMBUS or KeyBUS in the manuals depending on the exact model. The documentation implies that the protocol is different, but we were not able to obtain a KeyBUS system for testing.

Because the bus usually runs inside the wall, it immediately has a barrier against tampering. The primary alarm panel includes a special connector for directly attaching a PC or network card to the system, referred to as the PC-Link. It performs some translation between the serial bus and the computer. This connector is also usually well protected physically. Due to maximum wire-run length requirements, system modules or line amplifiers are sometimes positioned in other locations in a building which might not be as secure and might allow for unnoticed tampering. We found three other ways to gain access to these systems.


Caution: Lithium battery cannot be replaced.*
WARNING
High voltage. Disconnect AC power and telephone lines prior to servicing.
*Danger of explosion if battery is incorrectly replaced. If the lithium battery stops working, return the circuit board to your supplier. Batteries may cause a fire when in contact with metal. If you need to dispose of the circuit board and/or the lithium battery, wrap the battery in non-conductive tape. Check with your local government for battery disposal regulations. Please see Installation Manual, "Lithium Batteries" section.
WARNING
INCORRECT CONNECTIONS MAY RESULT IN IMPROPER OPERATION.
INSPECT WIRING AND ENSURE CONNECTIONS ARE CORRECT BEFORE APPLYING POWER.
PC-Link Connector
JACK SIDE
SI
SO
BOARD SIDE
UA016
WARNING: All circuits are classified for UL Installation as power limited/Class II power limited, except for the battery leads, which are not power limited. Please see Installation Manual Section 2 Installation & Wiring. A minimum 1/4" (6.4mm) separation must be maintained at all points between power limited wiring and all other non power limited wiring.
EGND
T-1
R-1
TIP
RING
AC
AUX
SAUX+
BELL
PGM
COMBUS
RED BLK YEL GRN
Z1 COM Z2 Z3 COM Z4 Z5 COM Z6 Z7 COM Z8 Z9 COM Z10 Z11 COM Z12 Z13 COM Z14 Z15 COM Z16
120V 60Hz UL-LISTED
UL Listed Class II Transformer 16 V @ 40 VA Recommended: DSC PTD1640U
Do not connect transformer to receptacle controlled by a switch. The transformer must be UL Listed and have a restraining means.
BELL LOOP 700 mA MAX
COMBUS TO ALL MODULES
Refer to the Installation Manual for detailed information on wiring.
BE SURE TO OBSERVE POLARITY WHEN CONNECTING POLARIZED SIRENS OR BELLS
TELEPHONE CONNECTION
TO GROUND CONNECTION
BRN
GRY
GRN
RED
OUT TO ESCORT4580 MODULE
INCOMING LINE FROM TELEPHONE COMPANY
RJ-31X Telephone Plug 26AWG
GROUND CONNECTION
Tighten nut to break paint and make a good connection to the cabinet
Nut
Lock washer
Nut
Lock washer
Star washer
Cabinet
Bolt
Ground wire from building electrical installation
RED
BLK
BATTERY 12 VDC MIN, 2 x 7Ah

As with the Lenel OnGuard system, DSC supports a variety of card readers and several standards for accepting data including Clock-and-Data and Wiegand. As noted in the 2008 paper, the Clock-and-Data protocol is fundamentally insecure and any information going over the wire, including card and pin numbers, is vulnerable to recording and replay. We found that many readers had tamper circuits available and did not use them, but a significant number did not even have the option, making it easy for a potential attacker to record data on the wire as shown in the 2008 paper. Because the systems we tested were mostly configured with proximity cards, they are even more vulnerable to cloning than the University ID cards were in the 2008 report. Though we did not attempt to buy one, cloning devices are available from China for as little as $100 or built for as little as $30.[4] Cards can also be spoofed with the proper equipment[5], similar to the way a flux generator can be used for magnetic cards.

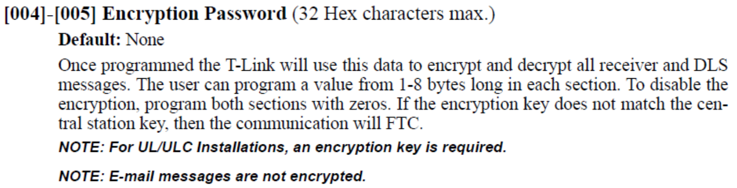
Attack Surface

The new attack entry method that we studied for the DSC system was the PC-Link. The PC-Link is designed to be used with Microsoft Windows-only software released by DSC called DLS, through a direct serial connection or a network module. The network module can also operate in standalone

[4] Brand name copier: http://www.corporatearmor.com/product_info.php?products_id=3582 (MSRP: $5000, Listed: $2500), Chinese knock-off: http://www.keymam.com/product_view.asp?pid=1632, Build it yourself: http://www.proxclone.com/reader_cloner.html

[5] http://www.proxclone.com/spoofer.html

mode, which allows the system to send email when specific events happen, but does not allow control messages or configuration to be sent back to the security system. The DLS software allows the user, from a computer, to configure any option they could access from the system keypad. It uses a configurable Downloading Access Code and Panel ID Code for authentication, but by monitoring the connection between the panel and DLS, we found that both are sent in without any form of encryption. For systems that connect over the Public Switched Telephone Network, installers can also configure the system to answer the phone on a dedicated phone line or cellular link or after a particular pattern of rings for a shared phone line. The system can also be set to require a local user to enter a code on the keypad to enable the dial-in for 60 minutes at a time.[6] The T-Link supports the use of a 128-bit encryption key, but because it must be entered manually from the keypad using hexadecimal characters, the option is rarely used.[7] The DLS software manual claims an additional security feature is that it can only be programmed using the Central Monitoring Station equipment as a proxy.[8] Despite that claim, we have found that the DLS software actually *can* connect directly to the T-Link module without the use of Central Monitoring Station equipment.



[004]-[005] **Encryption Password** (32 Hex characters max.)

Default: None

Once programmed the T-Link will use this data to encrypt and decrypt all receiver and DLS messages. The user can program a value from 1-8 bytes long in each section. To disable the encryption, program both sections with zeros. If the encryption key does not match the central station key, then the communication will FTC.

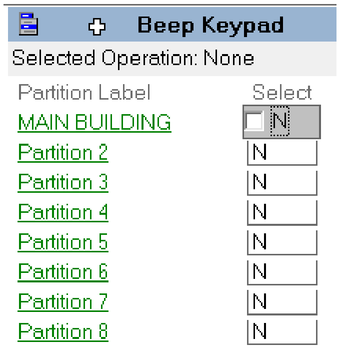
NOTE: For UL/ULC Installations, an encryption key is required.

NOTE: E-mail messages are not encrypted.

Manual explaining encryption key option. FTC means Failure To Communicate with Central Station. UL installation means when the system is used as a fire alarm. Manual does not specify what happens if key is wrong in direct connection mode

Practical Attacks

While DLS does not have its own registered port, we found that messages include distinctive payloads. We developed a SNORT rule to detect DLS connections even if the port has been changed. Once the communication port has been found, the major attack that we found these security systems to be vulnerable to is replay attacks. For a harmless example, DLS includes a feature for locating which keypad is where by making each one beep individually. We were able to intercept (using Wireshark) and record this command from DLS to the panel and play it back successfully. A variety of door locking mechanisms are compatible with this system, some which use current-flow to unlock and others to lock, so there is a configuration option to reverse the "polarity" of the locking mechanism for each



Beep Keypad

Selected Operation: None

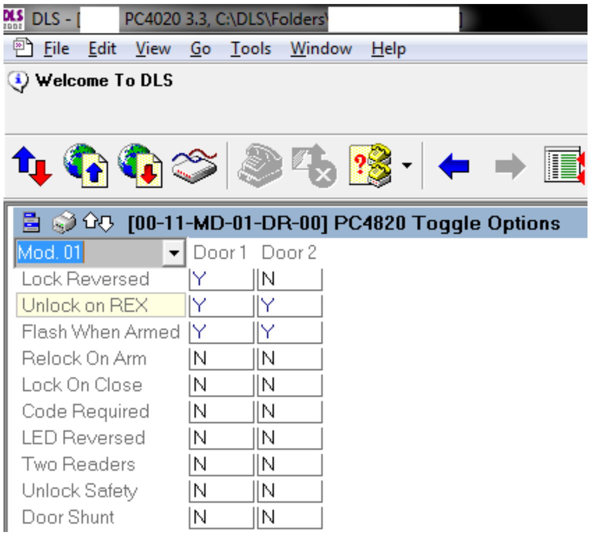
Partition Label	Select
MAIN BUILDING	□ N
Partition 2	N
Partition 3	N
Partition 4	N
Partition 5	N
Partition 6	N
Partition 7	N
Partition 8	N

[6] While not the focus of our research, in an informal survey we found that it would not be very hard to get users to enter this key combination by simply calling them and pretending to be from their alarm company. The names of the alarm companies that many people use are posted on a yard sign or window stickers. A significant number of people said they would not even know the correct name of the company themselves.

[7] Personal conversation with a professional system installer. There used to be software for configuring the T-Link over the network, but it was very hard to set up and support was discontinued.

[8] "The DLS software cannot communicate directly to the T-Link modules on the network. There must be a DRL-IP line card or Reporter IP software to route the T-Link communication."

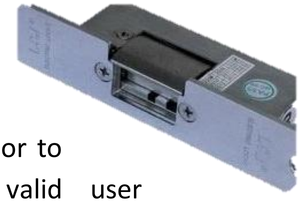
door.[9] We were successfully able to replay a command to reset the polarity of a door to be unlocked until a valid user attempted to get in and then to lock for 30 seconds. Besides for allowing potentially unauthorized access, this causes major annoyances for legitimate users.


DLS - [[redacted] PC4020 3.3, C:\DLS\Folders\ [redacted]]

Welcome To DLS

[00-11-MD-01-DR-00] PC4820 Toggle Options

Mod. 01	Door 1	Door 2
Lock Reversed	Y	N
Unlock on REX	Y	Y
Flash When Armed	Y	Y
Relock On Arm	N	N
Lock On Close	N	N
Code Required	N	N
LED Reversed	N	N
Two Readers	N	N
Unlock Safety	N	N
Door Shunt	N	N



The primary defense mechanism we found for a T-Link card that is not used for Central Office communication is to put it behind a VPN concentrator or use other network level access control and encryption. A centrally-monitored system should have the existing encryption key set (because we were not able to obtain Central Monitoring equipment early enough in the project, we were not able to test the security of the implemented encryption scheme). Systems with DLS configured should not use the default DLS password (1234) and should not be accessible over the internet. The Downloading Access Code and Panel ID Code should be changed from the default values. Home users and receptionists and staff should be trained never to follow the instructions of anyone who asks them over the phone to do something to the alarm system.

Crestron

Crestron manufactures systems for home and business audio/video control and for home automation. Crestron systems can be controlled from dedicated hardware control panels and/or from computers and mobile devices over a network. We will focus on the latter method.

According to the University Of Maryland Division Of Information Technology's Classroom Support Office, there are 255 General-Purpose classrooms on campus with classroom technology installed. All of these rooms use Crestron systems for controlling projector power and input sources, most use the systems for Projector Screen control (e.g. up/down), and many use them for lighting control as well. Most of the systems at the University are controlled from the classroom's computer in the front of the room, though some are controlled from

[9] For example, to unlock most electronic mortise locks, electronic crash bars (both common around the University of Maryland) or electronic strike plates, current is applied (fail-secure), while to unlock an electro-magnetic lock, current is removed (fail-safe).

wall-mounted or desk-mounted touchscreens. We have found that all rooms which are controlled from the instructor's computer have public IP addresses and are completely open to the Internet.

The University is using a version of the Crestron control software called XPanel. We will focus on it, but other versions likely have similar issues.

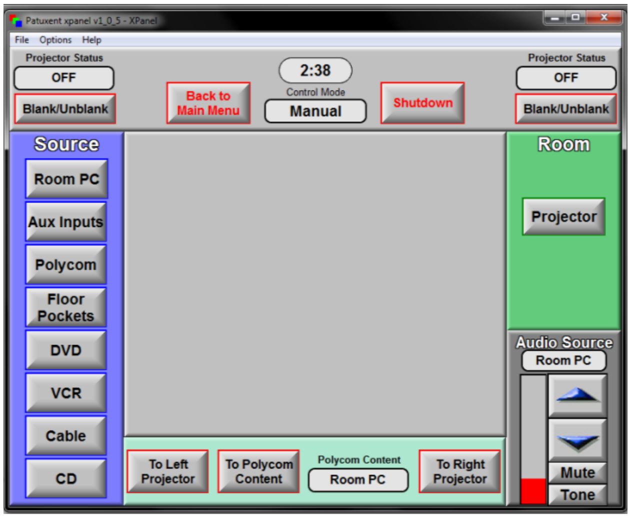
Possible Attacks and Consequences

There are a few main attack types against the Crestron systems that must be considered. The first is a Denial-of-Service, wherein a malicious user sends malformed or otherwise useless commands to the Crestron controller that cause the controller's software to crash or cause the controller to be unresponsive to legitimate requests in some other way. The second type is malicious sending of real commands to the controller to cause it to do actions that the instructor in the room does not want, for example, to switch to campus cable at full volume during an exam or to shut of the projector and the lights during a lecture. The latter possibility is particularly bas because of the projector's built-in 5-minute (average) cool-down timer which prevents the projector from being turned back on immediately and thereby disrupting class. A malicious student could bring all classes in Technology Classrooms to a halt by using a script to send multiple commands to every Crestron system on campus.

A third possible attack, much less likely though potentially much more damaging, is attacking Crestron units that control other systems like phones and/or cameras. This could lead to information leaks by an outside user connecting to phones or cameras and spying on conference rooms, meeting rooms, or lecture halls.

Practical Attacks

The simplest attack requires one-time physical access to a room (or several rooms) equipped with XPanel software on the instructor's computer. Most instructors we have observed will log into the classroom computer and leave it unsupervised for a few minutes at the beginning or end of the class period. It is trivially easy to copy the "Program Files\XPanel" directory to a USB device and use it from any network-connected computer. The Crestron software uses a template file that describes what the control screens look like so it may be necessary to visit a few classrooms and gather a representative sample of Crestron application directories. The only additional requirement is to know the IP address of the Crestron controller you wish to connect to. However, this is also easy because many of the controllers have DNS



XPanel running successfully on a research computer in Silver Spring, MD entries of the form “av-ctrl-<BLDG><ROOM>.umd.edu” and a port scan on the University network for the Crestron control port will turn up the rest.

Some Crestron software is also available on various anonymous open FTP sites, though not the software used by the University.

Using the first attack vector and running packet captures on the results, we attempted to analyze the Crestron protocol to determine whether attacks that blindly replay captured codes will work to send commands to the Crestron system. We found that the Crestron system uses a proprietary binary protocol but does have some clearly defined data packets for particular operations, and occasionally contains some plaintext for display on the control panel screen. While we were unable to finish this task due to scheduling issues of getting access to classrooms with Crestron systems we could test, based on the data that we collected, we are fairly confident that the Crestron systems are vulnerable to replay attacks.

Prevention Possibilities

It is almost impossible for someone who is not a Crestron-registered dealer and installer to access Crestron system manuals. Even most Crestron system owners cannot view most of the manuals for the products they own. While this does provide a small layer of Security-Through-Obscurity, there are still attacks, such as ours, that can be carried out without access to the manuals.

The Crestron systems used by the University do offer industry-standard SSL for XPanel ActiveX control. However, the University is using the Windows (and Mac) native applications, which do not seem to support SSL. Additionally, the SSL protection only prevents eavesdropping and modification at the channel level, but does not prevent an attacker from masquerading as a legitimate user, downloading the XPanel ActiveX control, and attacking the system using it. According to Gerry Sneeringer, the Division of Information Technology’s Director of Security, the Crestron manual does say to set a configuration password and to use a VLAN for Crestron traffic. However, it recommends the VLAN as a way to deal with congestion, not with security. He says that the University will be implementing VLANs to protect the classroom Crestron controllers from attacks.

To prevent the replay attacks that we believe are possible, the simplest thing Crestron could do would be to implement some kind of one-time code system used to hash every request. However, this may not be practical for systems that are supposed to be controlled by mobile devices which may have limited processing capabilities. Another option would be to implement a connected device whitelist. However, this would also cause problems with mobile device control, especially if a non-technical user has to add a new device or if the only authorized mobile device is lost, stolen, or broken. Another solution could be requiring a username and password, though that has the traditional problems associated with per-user credentials.

Additional Notes

Some Crestron systems, such as the controller in the School of Architecture, Planning, and Preservation’s auditorium, use a four-digit PIN number that must be entered before the system can be used. If Crestron systems are, as we believe, vulnerable to practical replay attacks, we would like to test if PIN-protected systems are also vulnerable. In other words, does the PIN only protect the GUI of the controller or does it protect the entire system?

E-Z Pass

E-Z Pass systems are used by 24 tolling agencies in 14 states, mostly on the east coast, for electronic toll collection for highways, bridges, and tunnels [1]. In 2011, 22.5 million transponders were used for almost 2.5 billion transactions, making E-Z Pass one of the most heavily used electronic toll collection systems in the United States. According to E-Z Pass IAG head P. J. Wilkins, E-Z Pass processes over 50% of tolls in the United States [2]. E-Z Pass tags are battery-powered RFID tags and are usually inside small windshield-mounted plastic boxes. Most toll plazas set low speed limits for E-Z Pass lanes, usually 10-15 mph due to the narrow width of the lanes, but E-Z Pass is actually designed to work at speeds as fast as 100 mph and many toll plazas have been retrofitted with wider lanes to allow speed limits of up to 55 mph. Some toll roads, including Maryland’s Route 200 (Inter-County Connector) use “Open-Road Tolling” with E-Z Pass readers and cameras positioned on gantries over the road without the use of any tollbooths.

E-Z Pass transmitters broadcast in the 915 MHz ISM radio band (nominally centered at 915.75 MHz [3]). They use a proprietary protocol, colloquially called “IAG,” which sends 256 bit packets at 500 kbps. The data is sent using Manchester Keyed Carrier encoding [3]. The protocol was designed by Mark IV Industries (now Kapsch TrafficCom IVHS), the maker of E-Z Pass tags. The implementation details are supposed to be a trade secret, shared only with toll agencies that use Kapsch tolling systems. (See “Recent Updates” section below for changes to this.)

E-ZPass Antenna on MD 200

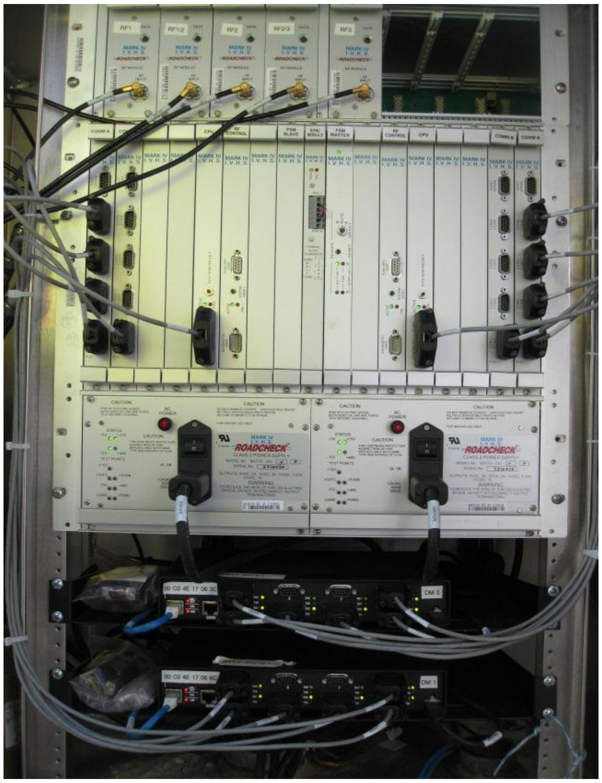
While E-Z Pass software and most specifications are not officially available online, specifications and other documents actually are available, in several locations on the internet, [redacted] the Internet Archive’s Wayback Machine [4], [redacted]. In particular, many reports, construction notes, and equipment manuals are available, including equipment rack layouts, configuration scripts, and internal communications. However, in the past few months, an increasing number of E-Z Pass documents and specifications have been made public due to E-Z Pass’ attempts to become a national standard. This has been beneficial to use because we have been able to analyze these documents as well as the ones we collected from other sources.

The E-Z Pass Transponder and Reader

According to the interagency information exchange specification files, a tag is uniquely identified by the a) Tag Agency ID (7 bits) and b) Tag Serial Number (24 bits) stored on the tag.

According to Reciprocity implementation agreements, the E-Z Pass reader attempts to verify the genuineness of an E-Z Pass tag by trying to read the tag as many times as possible. For gated toll lanes, there are expected to be approximately 100 handshakes between the reader and the tag [5].

During each handshake, the tag's identifying information is read, a one-time use ("nonce") number is written into its memory, and the nonce is then replayed and verified. If the verify step does not occur, the transaction is flagged as "programming unverified". If the write step does not happen, the transaction is flagged as "programming failed". These processes are designed to prevent accidental reads of nearby tags, but have the side effect of making it difficult to produce a counterfeit tag which may not meet the same standards. Note, however, that transactions with failed write or verify steps are still processed for payment collection. This could allow an attack perpetrated via a fake tag which might be easier than reprogramming a real tag with a new serial number.



E-ZPass "Badger" Tag Reader on MD 200. Visible in the bottom of the picture are the network serial converters used to connect the radio to the lane controller hardware.

According to E-ZPass specification documents, the E-ZPass Tag has storage space for a nonce, but all public and private E-ZPass documentation we have seen implies that the nonce is only read at the same toll booth, not at the next one, and that failure to read the nonce back from the tag is considered a soft failure, not a hard failure, and the transaction will be flagged but processed anyway.

Several E-ZPass documents referred to space on the tag for storing the entry point for closed-toll systems (i.e. "take a ticket at the beginning and pay what it says at the end" systems), however, the documents that we saw do not indicate whether this is a feature of the current system or only a feature that they wish they had but currently do not have. If this feature does exist, we need to determine whether it is vulnerable to changes, so that, for example, a malicious user could switch the tag to say a different entrance than the one which the vehicle actually used in order to pay a lower toll.

A highway that has upgraded its equipment is willing to sell us some of its old equipment for testing (with no questions asked) for about $7,000. If we want to research E-ZPass further, this may be a worthwhile investment.

E-Z Pass IAG is aware of the need for improved security in the E-Z Pass system. A 2008 Request-for-Proposal states that Proposers must describe the safeguards they have in place to prevent the use of counterfeit tags or any other means of bypassing the toll system [6]. The RFP also states that Proposers must specify how their tags will prevent unauthorized modification of data stored on the tag, such as the entry point for closed-toll systems, though there is no documentation of how the current tags do so. The RFP also requires that tags "shall not open readily" and "shall be resistant to the influence of any interrogating and decoding signal or medium" other than the intended tag reader (Section 2.6.5.4.3). However, there is no indication that the current tags meet these requirements either. Finally, the RFP defines several data fields which should be factory-set and not changeable later, even by the operating agency. The tag's serial number is included in this list, which would prevent a malicious user from writing someone else's serial number onto his own tag. However, like the previous ones, it is unclear whether this requirement is met by the current E-ZPass system.

We attempted to set up a radio to record E-ZPass radio transmissions. While we were able to record the presence of the E-ZPass signals, we were not able to process or interpret those signals. For legal reasons, we did not attempt to spoof an E-ZPass tag.

The E-Z Pass Network

E-Z Pass specifies that data is transferred between toll agencies using fixed-width plaintext files that are zipped and transferred between agencies [7]. The interagency reciprocity agreement states that these files are to be distributed at least once per day, if not more often. The files include:

- Lists of valid and invalid tag numbers, distributed from every agency to all other agencies.
- Lists of transactions, sent back to the appropriate "Home Agencies" for billing.
- Lists of transaction results, sent from each "Home Agency" back to the "Away Agency" at which the toll was charged.
- Lists of license plate numbers associated with E-Z Pass accounts, distributed from every agency to all other agencies to allow processing of tolls if the E-Z Pass tag was not properly read and a license plate picture was taken instead.

Note that there is no encryption or validation done on these data files. They are sent as zipped plaintext and the acknowledgements are sent back as zipped plaintext. This could be a major vulnerability. For example, a malicious attacker could artificially run up someone else's bill by sending additional transaction files. An attacker could also send a file to reactivate an old or stolen E-Z Pass tag. An attacker could also attempt to intercept and modify a file sent by a legitimate toll agency.

However, the current risk of tampering with interagency reporting is actually very low because the E-Z Pass agencies use a private non-routable Managed Frame Relay (MFRS) network. The network uses class-B private addresses (though it also spills over into a block allocated to T-Mobile) so it would require physical access to the Frame Relay circuits or to an E-Z Pass Customer Service Center in order to exploit this part of the system [8].

Recent Updates

As mentioned above, E-Z Pass is trying to position itself to become a national standard tolling protocol. To further this goal, they have published many of their previously private specification and implementation documents online, primarily for the purpose of sharing them with other tolling agencies. This has allowed us access to more documents than we previously had and may enable additional future work on E-Z Pass security.

On October 24, 2012, Kapsch TrafficCom IVHS announced that the protocol specification will be released for public access in order to encourage compatibility with other tolling systems [9]. This will allow better access to the specification for security research as well, without having to reverse-engineer the implementation.

The E-Z Pass Interagency Group is currently working with other Toll Agency groups, Solution Providers, and Government agencies on National Standards for Electronic Toll Collection. In the process of working on these standards, they have discussed some of the issues that we have discovered.

[redacted] However, since one of the current protections of the E-Z Pass data is its isolation from the public Internet by virtue of its use of MFRS, it will be interesting to monitor whether the new system improves, maintains, or worsens inter-agency communication security. For example, MdTA (Maryland Transportation) uses standard VPN technology to protect their data while transferring it over the public internet. The plan also calls for improving the existing transaction processing, payment processing, and file transfer processes.

Conclusion

The proliferation of technology designed to help make everyday tasks easier leads the average user to pay less attention to their digital footprint. Each of the vulnerabilities we discussed in this paper allow an outsider to monitor, control or otherwise tamper with a person's activities, property and even safety. We hope our research will lead to consumers paying more attention to their digital footprint and to companies building security as one of the pillars of their products, not an afterthought. People already pay attention to how their personal information is used on social networking sites and how it is made available to others on the internet. These systems should be no different.

References

[1] E-ZPass Interagency Group, [Online]. Available: http://www.e-zpassiag.com/. [Accessed November 2012].

[2] N. Bradley, "E-Z Roller," *Tolltrans,* pp. 24-28, 2012.

[3] Kapsch TrafficCom IVHS, "Badger Reader Datasheet," [Online]. Available: http://www.kapsch.net/ktc/downloads/datasheets/datasheets_allcountries/rf-field/Kapsch-KTC-DS-Badger?lang=en-US. [Accessed October 2012].

[4] E-Z Pass Interagency Group, "E-Z Pass Members Only Section," September 2008. [Online]. Available: http://web.archive.org/web/20080907060109/http://www.e-zpassiag.com/members.html. [Accessed September 2012].

[5] E-Z Pass Interagency Group, "Reciprocity Agreement II: Addendum II," April 2001. [Online]. Available: http://www.e-zpassiag.com/images/agency_portal/official_documents/Reciprocity%20Agreement/Reciprocity_Agreement_02_00.pdf.

[6] E-Z Pass Interagency Group, "Request for Proposals to Furnish and Provide Electronic Toll Collection Technology and Associated Subsystem Components and Services for the Operation of the E-ZPass System, Section 2.6.2.7," March 2008. [Online]. Available: http://www.e-zpassiag.com/images/agency_portal/official_documents/MarkIV_Kapsch/NGcontract2011/RFP/2782%202%20of%202/IAG%20RFP%20pdfs/1-IAG%20RFP%20Sections%201-5%202008.pdf.

[7] E-Z Pass Interagency Group, "Interoperability File Specifications," [Online]. Available: http://www.e-zpassiag.com/interoperability/87-interoperability/file-specifications/332-file-specifications.

[8] E-Z Pass Interagency Group, "Inter CSC Reporting File Appendix: IP Addressing," [Online]. Available: http://www.e-zpassiag.com/images/agency_portal/official_documents/IAG-Circuit-IP2011-11-06.xls.

[9] Kapsch TrafficCom IVHS, "Press Release: Kapsch to Release E-ZPass Technology," 24 October 2012. [Online]. Available: Kapsch to Release E-ZPass Technology. [Accessed November 2012].