

SECURITY VULNERABILITIES IN THE TOLLING INDUSTRY

Donovan Young

Senior Toll Consultant – Traffic Technologies Inc.

IBTTA Denver 84th Annual Meeting & Exhibition
September 11th – 14th 2016

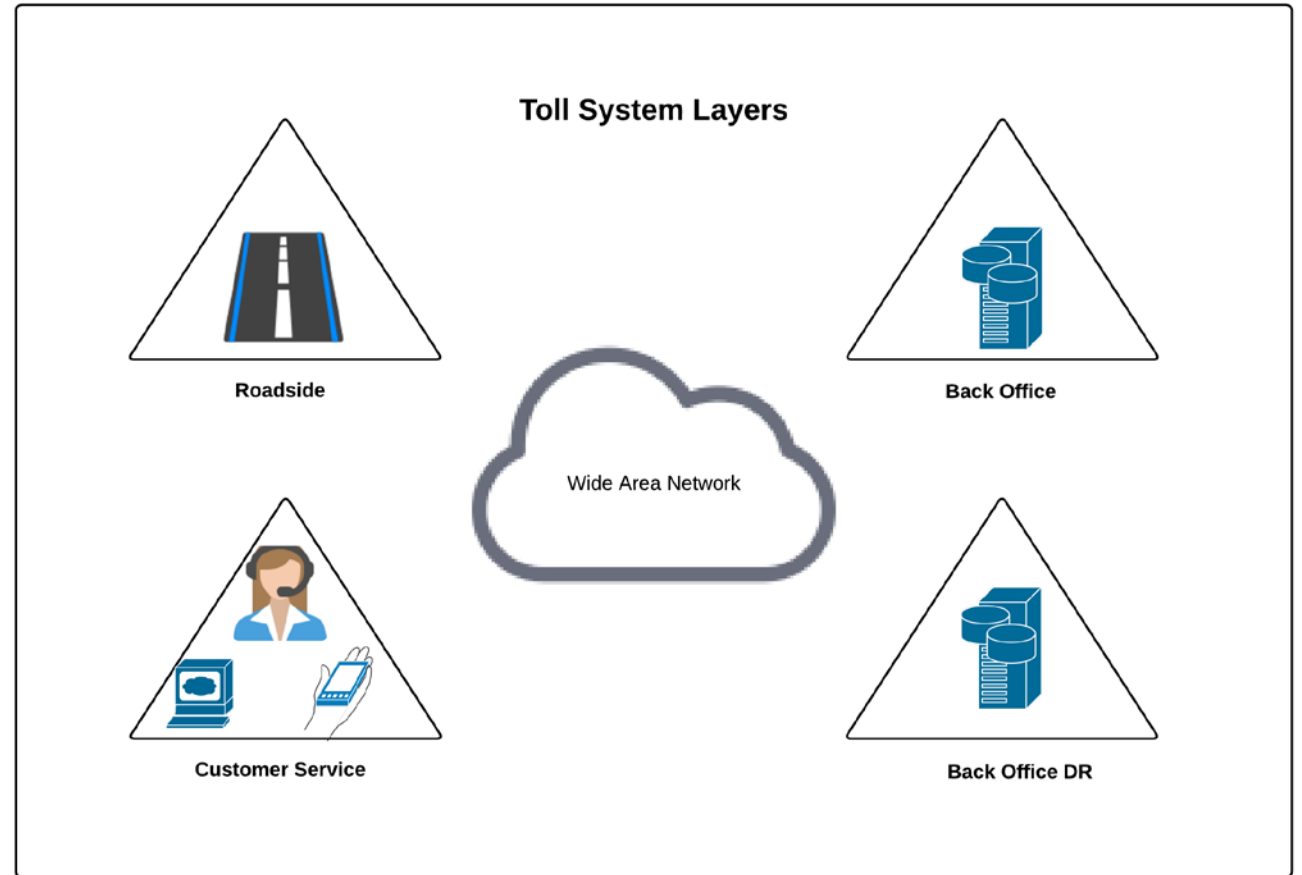


INTRODUCTION



LAYERS OF A TOLL SYSTEM

- Roadside Components
- Back Office System
- Customer Service



ROADSIDE COMPONENTS



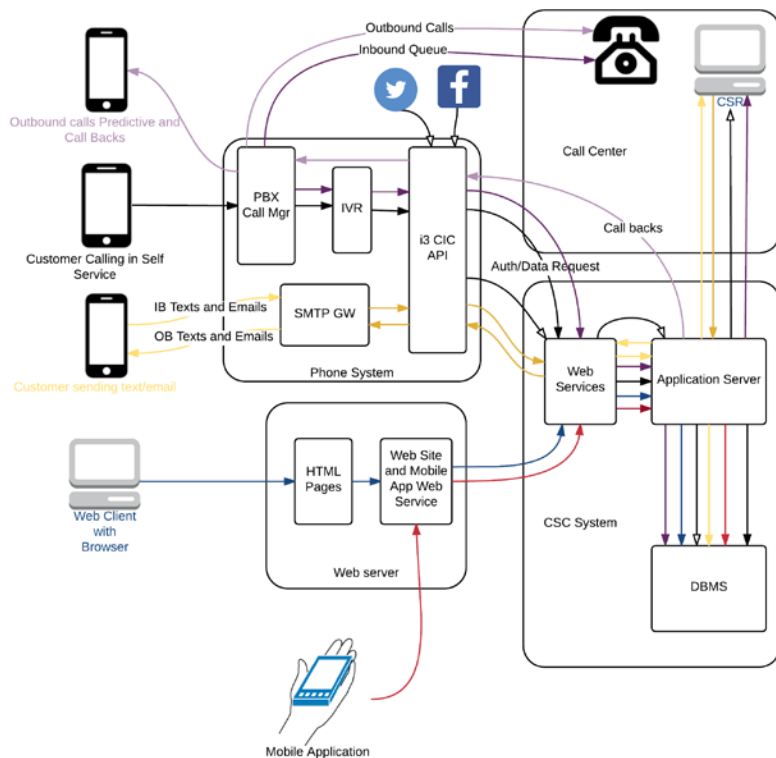
- Gantry Equipment
- Toll ITS
- Network
- Toll Facility Hosts
- Link to Back Office

BACK OFFICE SYSTEM

- Hosts
- Network
- Data: Customer & Proprietary Information



BACK OFFICE SYSTEM



Interfaces

- CSC Web and Mobile App
- Bank
- Interoperability
- Collections
- DMV
- Courts and Registration Holds
- Mail house
- Transponder/Retail

CUSTOMER SERVICE

- Call Center
 - Phone (IVR – CSR)
 - Walk in Center
 - Mobile Walk up
- Web
 - Mobile App
 - Email & SMS
 - Social Media
 - Web chat



SECURITY VULNERABILITIES AT EACH LAYER



Roadside

- Toll ITS - CCTV & DMS
 - ❑ Public facing
- Cabinet/Hub Security
 - ❑ Access to cabinets or hubs means access to the network and equipment
- PII – License Plate and Transponders
 - ❑ Transactions in Flat Files
- Link between Roadside and Back Office
 - ❑ Higher risk if done over the public Internet
- Network
 - ❑ Any breach of the roadside network
 - ❑ Remote Access

SECURITY VULNERABILITIES AT EACH LAYER

Back Office

- Hosts
 - Logins
 - Patches
 - Unmonitored open ports & modules
- Network
 - Internal and external
- Data
 - PCI – Credit card information
 - Personal Identifiable Information (PII)
License Plate Data, Financial Data,
Customer Data
 - At rest & In motion



SECURITY VULNERABILITIES AT EACH LAYER



Account #, Transponder # or Username

PIN Save this ID


Sign In

Create New Account
Follow Us!

Reset PIN
Unlock Account

More Info

FDOT SunPass® is a registered trademark of the Florida Department of Transportation.



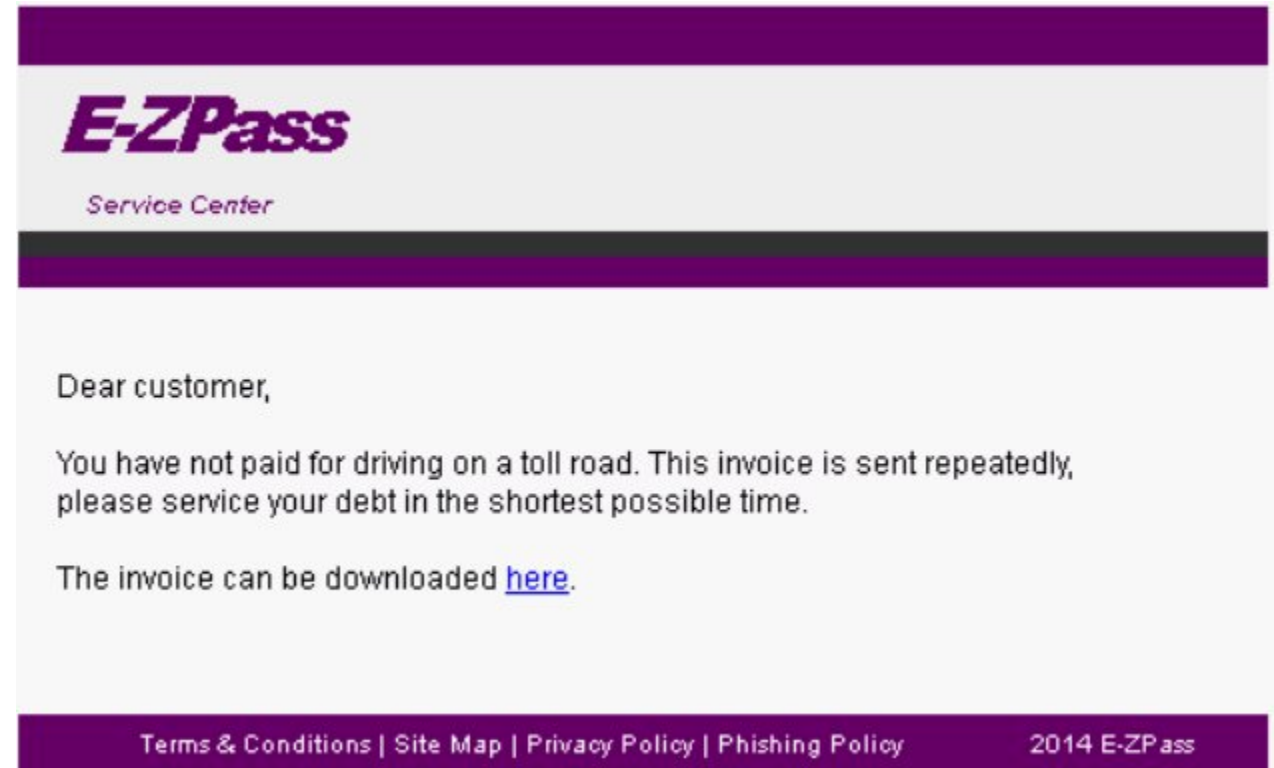
Back Office

- Interfaces

- CSC Web and Mobile App
- Bank
- Interoperability
- Collections
- DMV
- Courts and Registration Holds
- Mail house
- Transponder/Retail

CUSTOMER SERVICE

- Phone & Walk up locations
 - Social Engineering
 - Mobile locations – Less security
 - Walk ups that take cash
- Email & Web chat
 - Phishing
- Theft
 - Credit card numbers
 - Transponders
 - Free Tolls



The screenshot shows an email from E-ZPass Service Center. The header features the E-ZPass logo and 'Service Center' text. The main body of the email reads: 'Dear customer, You have not paid for driving on a toll road. This invoice is sent repeatedly, please service your debt in the shortest possible time. The invoice can be downloaded [here](#).' The footer contains links for 'Terms & Conditions | Site Map | Privacy Policy | Phishing Policy' and the text '2014 E-ZPass'.

FUTURE TOLL SOLUTIONS



- Improved encryption and decryption speeds
- Network as a Service
- Security as a Service
- Cloud
- More advanced IVRs

CONCLUSION

The goal should be to reduce the number of vulnerabilities because most Toll Agencies don't have a full time security staff to monitor and audit all of the layers of the Toll System for security risks and incidents. Complete reliance on the Toll System Integrator, without oversight, is not recommended.

```
struct group_info init_groups = { .usage = ATOMIC_INIT(2) };
struct group_info *groups_alloc(int gidsetsize){
    struct group_info *group_info;
    int nblocks;
    int i;

    nblocks = (gidsetsize + NGROUPS_PER_BLOCK - 1) / NGROUPS_PER_BLOCK;
    /* Make sure we always allocate at least one indirect block pointer */
    nblocks = nblocks ? : 1;
    group_info = kmalloc(sizeof(*group_info) + nblocks*sizeof(gid_t *), GFP_USER);
    if
gro
gro
gro
ato

    if (gidsetsize <= NGROUPS_SMALL)
        group_info->blocks[0] = group_info->small_block;
    else {
        for (i = 0; i < nblocks; i++) {
            gid_t *b;
            b = (void *)__get_free_page(GFP_USER);
            if (!b)
                goto out_undo_partial_alloc;
            group_info->blocks[i] = b;

```

