PLAY DATE AT THE AIRLINES

VERSION 1.1.0

AVI ZAJAC

CONTENTS

PREFACE

Back in March 2017 I intended to submit a Call For Paper (CFP) to DEF CON on airline security. Why? I absolutely love airlines and air travel, want to help fix it, and I wanted to see if I was capable of writing something that could be presented on a stage. Especially with it being my fifth year of DEF CON it was a challenge to myself. At first it was a solid two dozen or so pages scattered in every direction because I really want to help with every area I saw issues in. After polling, asking what folks would be more interested in, I narrowed it down to twelve or so pages and asked people to review it.

It was after a final lovely review from a wonderful DEF CON CFP review board member (who would have had to omit from voting on mine if I had submitted) that I decided, with all other potential issues legally with it, to not submit.

This series was born out of the original CFP I had. I have narrowed down the focus to give context to an issue that I believe needs to be looked at in a different light than the current state of audits do. Airlines and airline employees work around current audits, not for them. This is something I am deeply in love with, something I'm motivated to do, and happy to talk about with others.

Current and former airline employees can't do this alone to fix the problems.

So hopefully you'll speak up too.

Finally for acknowledgements I'm thankful to all those who reviewed my CFP (there was much mix debate and review on the length of the proposal). It was a lovely first exposure to working on one. Much love to my airline family from all the airlines they belong to, for always having supported me from the first day I joined to even now. Laughing and having joyful yet serious conversations about airline things while writing the CFP really inspired me to keep on writing for them. Hopefully by addressing the issues they care about here I can help make their lives easier, secure, and safer than with the current state of the waiting game.

AVI AIRLINE TIMELINE

I have an odd habit of ending up working at places where I'm very obsessed with figuring out how things work, find where the systems in place fail and why, and find more cute things inside of it to obsess over. That included the airlines.

I worked from 16 March 2015 to 16 March 2016 officially in the airlines.

Starting out as a customer service ticket counter agent I was pulled a week or two later to replace the outgoing person who was the station training compliance coordinator. I took over while also becoming for two months the primary station ops agent. I also got recruited and became an emergency response team member and then became the emergency response coordinator maintaining emergency plans and the business continuity for my station.

Outside of other things I was the baggage service champion for my station, was the primary cargo acceptance agent, became an instructor for cargo and new hires. I was also tasked with the transition workforce wise of the legacy system to the new system at my station. That was amusing to me because I loved the legacy system and remained using it for certain aspects of the job. I'll explain why later.

At one point I handled and did the regional safety minutes and reports for my region. I also dealt with all of the irregular operations (IRROPS) like that one diverted flight I got alone at night while also working on two of my own delayed flights. IRROPs loves me and I loved IRROPs, too.

My time management skills was a core part of how I was able to maintain and keep going through the system into various trainings for different positions simultaneously. A typical work day consisted of baggage service champion duties, training compliance work, instructor duties with creating or updating new manuals, informing agents of updates to policies, ticket counter, gates, working with station ops, and whatever else we needed that day.

That and in my down time finding cute stuff to play with.

1 - INTRODUCTION

Disclaimer: Everything written here has been done either in research, observance, and finding publicly available documents, forums, and so forth on major search engines. To my knowledge there is no SSI contained in any of these sections. All information found here can be easily sought and found online. Citations can be made available if requested.

While you may be a frequent flier or are in the airlines and feel like you already know the linguistics of the airlines I do recommend reading the following list on airline vocabulary provided for these sections. That is to ensure we are on the same page. If this is an entirely new concept of what occurs once you enter through the airport doors this is a requirement to understand the following sections.

AIRLINE VOCABULARY

PNR *(Passenger Name Record)*

This is the 6-digit alphanumeric series of characters on your boarding pass and reservation information. This is a record of your information in the airline's database for easy reference. Notes and logs from the system related to you go onto the PNR. Verify on your boarding pass that you see a PNR number and an eTicket number.

eTicket (Electronic Ticket)

This is your reservation number. A 13-14 digit number. If your boarding pass does not have an eTicket number (even if you see a PNR number on it) your PNR is *out of sync* and needs to be *resynced*. Military and those booked by third parties tend to have out of sync PNRs frequently due to various issues (e.g. payment not received to the airlines from the third party).

APIS *(Advanced Passenger Information)*

Part of the TSA's Secure Flight Program this is for international PNRs.

Non-rev/NRSA *(Non-Revenue Seat Available)*

Either an employee, retiree, family member on the employee’s flight benefits, or have a buddy pass from an employee flying for leisure for free or at a discounted rate (e.g. ZED fares).

Positive space/NRPS *(Non-Revenue Positive Space)*

An airline employee who must fly for business related issues related to their airline. NRPS is applied to deadheads, people flying for training, conferences, etc.

Deadhead

Flight crew member flying to another city so they can go to work. For example you may deadhead a crew from City A to City B so a flight from City B can leave. If there is no deadhead crew going to City B there will be no crew available to fly that (or any) flight. This is called *repositioning*.

Jumpseater

An off-duty crew member using the spare jumpseat when there are no more passenger seats available for leisure travel (though many do this to commute to work, too, which can be confusing with NRPS status which they are not under, this is classified as NRSA travel).

[Flight] crew

Pilots and flight attendants for a flight. If I am referring to other type of crews I will preface crew with a specific group I am targeting (e.g. BTW crew).

ATW *(Above The Wing)*

Covers all employees who work “above the wing”. They are the customer service agents at the ticket counter, the gate agents, the main station supervisors, station managers, and more.

BTW *(Below The Wing)*

Covers all employees who work “below the wing”. This includes ramp agents, station operation agents (ops), dispatch, fuellers, and more.

Contract of Carriage

Contract agreements between the airline and passenger. Defines your legal rights, liabilities, and further. All ATW airline employees by law must be able to define the Contract of Carriage to you by pointing you to the website or a mini brochure version of it provided by their airline.

Restricting and unrestricting flights

If you avoid online check-in (or your airline doesn't provide it) you may have experienced getting to the ticket counter too late. You have missed the *cut off time to check in*. This is stated in each airline's Contract of Carriage at what time that is (typically anywhere from 30-45 minutes prior to flight departure time for US domestic flights). What they did was *restrict the flight* at the gate to a single machine. That machine is now the sole machine able to '*touch*' this flight (e.g. passengers, bags). Smaller stations may sometimes be nice to you and *unrestrict the flight* so you can check in. At a hub though? (Essentially…) Never.

Closing and [re]-opening flights

A gate agent may have to *reopen a flight* (e.g. on the radio, "Reopen that flight," to that agent) in the event of a deplaning. If you've seen this occur before you may have seen a gate agent re-scan passenger boarding passes so they are *off* the flight (as opposed to being *on* the flight in the systems when they scan you onto the jetbridge the first time). When a flight departs they *close* the flight, essentially it is a fully completed flight thus nothing can be altered anymore. Benign sounding this has serious implications because it all relates to the *flight manifest*.

Passenger Flight Manifest

Every single flight has a manifest. There are various versions of it akin to "light" or "minified" manifests but essentially it must have everything on that flight on it. In the event of a crash or emergency this is automatically the first thing to be guarded and secured.

RELATED AGENCIES AND DEPARTMENTS

Department of Homeland Security (DHS)

A cabinet department of the U.S. federal government with their primary responsibility being public safety. After the 9/11 attacks the department was created and formed in late 2002, being the youngest U.S. cabinet department to date.

Transportation Security Administration (TSA)

A child agency to the DHS with authority over security involving air travel. They screen passengers and cargo at the airport in the U.S.

U.S. Customs and Border Protection (CBP)

A child agency to the DHS their primary goal is to prevent terrorists and terrorist weapons from entering the country. They're the ones screening passengers and cargo from international airports.

Department of Transportation (DOT)

A cabinet department of the U.S. federal government with their primary responsibility being transportation. Established in 1966 they began operating from 1967 onward.

Federal Aviation Administration (FAA)

A child agency to the DOT with authority to regulate any and all aspects of civil aviation. Established in 1958 once the DOT was established in 1966 they became one of the child agencies in it.

International Air Transport Association (IATA)

A trade association of the world's airlines, they formulate and establish the industry's standards and policies.

There are countless more whether by local municipality level, city level, state level, and so forth. All of them are crucial and create various rules that airlines must abide and follow by. Oftentimes this means they create a checklist of things airlines must do and so airlines will do things that they are told to do until they're told not to do that anymore.

With multiple agencies still being fairly recent historically, standards and policies changing after incidents, things change sometimes on the daily for airline employees with what they're told to do. This leads to much confusion as their new instructions may conflict with other active standards and policies by other agencies and so on.

This is a massive weak point and flaw, especially as someone who has seen this first hand by ensuring employees did their training (which does not necessarily account to much, either).

WHY IT'S SO HARD TO TALK ABOUT AIRLINE SECURITY ISSUES

When you start talking about security issues in the airlines, whether you're a researcher or someone who notices things, you're walking on very fragile ice. The largest issue for me to talk about this as a former airline employee is *Sensitive Secure Information* (SSI) - 49 CFR §1520.5(b). The shorthand for airline employees is that it is "a need to know basis" rule with plenty of terrifying penalties for failing to adhere to it.

Essentially if it's required in your job duties to know something, you have to know it. Otherwise you shouldn't know it. Any document that has SSI on it clearly states on it that it has SSI. If you have SSI it must be secured (if you find a document with SSI on it openly at the airport someone will be getting in trouble as neat as it may seem finding it).

To get a taste of why this is significant before we approach it again serving myself as an example I had a great amount of exposure to things with SSI due to having to do and know everything. *Some things that may seem fairly blatantly clear if you're observant as a passenger and talk about it is SSI for airline employees.*

Other issues outside of SSI are simply nondisclosure agreements and other documents you sign when you go work at the airlines due to the sheer amount of proprietary software and information you can get access to. An example is that the FBI has my fingerprints which is the deal I agreed to so I could get access to the *sterile area*.

2 - THINGS TO KNOW ABOUT AIRLINES

HACKERS? BUG BOUNTY?

Airlines have a goal to essentially transport as many people and cargo possible in an aeroplane to their destination and gain revenue. Having their issues pointed out whether customer service related to security flaws is something they despise for obvious economic reasons. It'd be a disaster revenue wise to keep passengers if all they hear is, "Massive security flaw found allowing anyone on the internet to do access all of their information on an airline's system." That and it's against federal law to essentially do anything to an airline due to air travel security.

They really do not like hackers. One notable example would be sidragon, aka Chris Roberts, who was banned by United Airlines and detained by the FBI in April 2015 followed by a search warrant.

Shortly after this incident United Airlines came out with a bug bounty program. Except it's a rather flawed bug bounty program with giving out miles instead of a cash payout, the limitations on what you're allowed to do are strict. A specific line that should be noted in their bug bounty program is:

> *"The researcher submitting the bug must not be a current or former employee of United Airlines, any Star Alliance™ member airline or any other partner airline, or a family member or household member of an employee of United Airlines or any partner airline."*

This limits those inside the airline from being able to profit off of bugs that they may potentially create which is understandable. I personally do not care for a payout as I have no desire or intention of gaining a profit by submitting bugs, as a former airline employee I want to help out with internal vulnerabilities so I can sleep knowing that passengers are safe and secure. Where can I report this to?

Nowhere.

NO INTERNAL BUG REPORTING

From my own research of trying to report vulnerabilities I discovered there was no internal bug reporting program. There were emails that led to nowhere in my attempts to reach out to the team developing it. It was not until I spoke about it to a developer at an in-person management meeting I attended on the transition to the new system that a few weeks later it was fixed.

With a time period of three or four months from when I discovered it this means that it was vulnerable most likely from whenever it was first pushed to my discovery of it. Since this experience I've learned and realised now many more things that I could have tried out, most of which would likely have worked. Without access to (or permissions) messing around with it myself there is no way to know. But I do know that it is not their priority because they are internal systems.

The FBI has their back, right? No need to worry for them.

As far as I am aware currently there is not a single airline with an internal bug bounty program or a place to report vulnerabilities to. I believe this is for several reasons whether it be they assume those working at the airlines aren't technically capable of understanding the applications and how they work, the bureaucracy that exists structurally employee wise, the entire airline family culture that exists, and believe instilling fear of breaking rules with consequences will fix potential issues.

FALSE SENSE OF SECURITY

When an employee undergoes training an instructor will state all the federal fines and prison time for doing various things to the airlines repeatedly. With the overall safety and security, PII, and other things employees have access to there are paragraphs after paragraphs of warnings on everything they do. Most folks are naturally not going to want to poke around or aren't bothered enough to do so.

In a personal experience I experienced an odd twist during training. We were warned but also taught how to look up frequent flier numbers by finding information on celebrities. Everyone I went to training with forgot how to do it since the Premier Desk can easily do that for you and tell you the information that you're requesting (upon them of course agreeing to provide it), but what about the folks like me who didn't? Not that it really matters because there are a slew of other ways an airline employee can get access to your information if they wanted to.

While researching things to support what would have been a talk I accidentally came across pages and pages of PDFs from various places with entries to several legacy systems. There are certain legacy systems like SABRE that are very common. SABRE is taught in hospitality, used by travel agents, etc. A non-airline person may not know if they've come across an exact entry-for-entry document of a specific airline or if the document has part of the entries.

Yet if you read these documents that are currently publicly accessible you can easily start getting a quick understanding of how the login system works with sine numbers, agent sines, duty codes, and whatever else is required.

To an airline keeping (non-airline) people out is more important to them than (non-airline) people knowing the entries and how it is set up. So long as no one else can't get access to it that's what matters. That and waving around the federal prison and fine warnings at employees, the moral taught is if someone does something wrong they'll go to prison and that's that. End of story.

That's pretty terrifying to think of for anyone else who is involved with security.

Especially since I did discover I was able get onto the entire system including any flight, restricted or not, in a web browser with full access. This was not fixed for a minimum of three or four months. Airlines must set up proper vulnerability reporting internally and not only regain the trust of their employees, but trust their employees will ethically disclose vulnerabilities, too.

United Airlines does have a feature now that allows an employee to submit issues with the application but it is not intended for security vulnerabilities, it's intended for glitches and bugs. In addition do employees really have time to report that weird bug they saw while rebooking customers that are yelling in front of them? No, because they'll do what they were told to do by everyone:

Right click and refresh.

3 - AIRLINE CULTURE AND COMMON ISSUES

AIRLINE FAMILY CULTURE

Have you ever been to the Smithsonian National Air and Space Museum in DC? I highly recommend it, they really go into depth throughout the exhibits of the commercialisation of air travel across the decades.

Why I bring this up is that air travel for commercial leisure is historically still fairly new and things are still being worked out. Outside of KLM in 1919, the 1920s saw commercial airlines springing up. The FAA was formally created into a child agency of the DOT in 1967. Over the last decades and even in recent times with the US Airways merger with American Airlines there have been a lot of mergers into what we know now as the primary largest legacy airlines: United Airlines, Delta, American Airlines.

This also means entire generations of airline families have occurred in this time. It is not uncommon for someone to work side-by-side with their parent, a grandparent, a great grandparent, maybe even more which is fascinating.

You tend to see people, especially with seniority, raving to one another fondly about the 'good old days' in companies they worked for prior to being acquired. The easiest modern day company to target would be United Airlines: employees refer to themselves by *'old United/UA'* or *'old Continental/CO'* rather than just *'United'*. This isn't fair, however, as you'll often hear the rundown of various companies through other acquisitions such as Delta of Northwest Airlines, the latest merger of US Airways employees into American Airlines, and many more.

Everyone who is or has been an airline employee is considered to be family, moreso if they come from the same (series of) companies. I am not sure how to define or describe this feeling if you have never been an airline employee or have never been a part of an airline family legacy, but there is a very strong intimate familial bond that forms amongst those in the airlines. I can attest that some of my strongest bonds I have ever made in my life so far have been my airline family, I love them all very much as if I have known them all my entire life.

The point to this is that there is at least some type of acknowledgement or immediate attachment to other airline folks. It may be because of things like the work hours: for trainings and for business an employee is likely going to be gone for weeks, more if they are above a regular agent. Employees cannot talk about their work (which is a familiar sentiment surely for those with government clearances) because of SSI to someone without the same *need to know* basis. The stress and constant change that's always happening builds up.

When airline employees get recruited into the airlines and undergo the training they are emphasised at at the need and ability to adapt to change easily. On the other hand for a lot of people that is easier said than done. Most struggle, then to throw into their confusion with conflicting information, that leads into a recipe for disaster with disgruntled employees who end up being apathetic to changes (or the seniority gets to their heads).

Really though it's nice being able to talk about your frustration with someone else who just gets it, right? Plus it's really fun to talk with someone who understands your life completely whether it be about how awesome your regular* was and that you can't wait to see them next week or how awful that one flight you worked was.

*=**Regular**: A frequent flier typically with status whom employees handle frequently

SPEAKING A 'DIFFERENT LANGUAGE'

People inside of the airlines trust each other a lot due to the nature of their work with SSI and other restrictions. Due to being unable to speak to anyone else about their issues/complaints at their jobs their airline colleagues are their second families hence the airline culture that exists within employees.

With all the various systems and components that go into a passenger getting onto an aeroplane to their destination there is a lot of vocabulary and things viewed as intimately 'just' inner airline culture references. Essentially they feel like they speak a different language with airline lingo and jargon assuming (rightfully so for most) passengers do not know what they are talking about.

There is a sense pride to that, too. That idea is played out in the form of training new hires to not use airline jargon around passengers lest they may confuse the passengers (which is typically true) leading to openly talking about things without fear of being understood (which is the mistake).

If you have ever had an agent kind of blabber off into their own world with maybe even another colleague blissfully and completely ignoring you while they rebook you that's why.

SMALL STATIONS VS. HUBS

The differences between those who work at a small station to an international hub are staggering. It creates a literal divide internally of what employees are capable and not capable of doing. Employees at smaller stations tend to do multiple roles (e.g. ticketing and gates) compared to hubs where people rarely, if ever, switch in their careers to a different area of the airport. This is due to the highly competitive seniority bids for schedules and departments in addition to simply having more people working there. They also have more *ready reserve* (RR) employees who may only work once or twice a month as a backup to full-time and part-time employees on vacation and such.

Yes, you're probably correct if you're thinking on this while reading. Due to having limited to no exposure at all to other duties and positions most employees at hubs have a very limited knowledge set outside of their daily functions if they have that knowledge set at all.

Travel tip: Never trust your ticket agent if they say, "Your flight is okay," if you know that other flights are delaying. Whether it's because they legitimately don't know or that they don't want to deal with you, they do not understand how the gates work at all. It's a foreign concept for them and they're passing it onto the next person to deal with you.

TRAINING ISSUES

It may feel like I am stuck in a loop repeating this but I cannot emphasise this enough: they are constantly changing information whether by federal or international requirements, or for internal reasons. It becomes easily very hard to keep up with for most employees because when the day ends they want it to end. That said there is a massive variance in what people know whether it’s a lack of knowledge or only recalling a previous standard.

While most industries have their employees go under quite a lot of training also I cannot emphasise enough that airline employees get a ton. I know, I was the one that had to ensure everyone did them. They had to deal with me chasing after them when they didn’t do their trainings. I know first hand that it is overwhelming to most employees at the amount of training they get. It may feel unreasonable to employees as to how they are expected to remember every single edge case, most being very infrequent if not rare (or never happen in their entire lifetimes even).

Of course one can and should argue that they should know these things if they've done the training. There’s no excuse, isn’t that why they were hired? Except at the end of the day though they're also human, they want the work day to end so they can get home, like most other people do. Most can do their jobs, do it well, and that's what matters to them. Who really cares about that edge case? (I do but that is not the point of this).

It's one more thing to complain about with your fellow colleagues, right?

OUTSOURCING PAINS

Airlines are outsourcing, especially at smaller stations or departments (e.g. baggage service, ramp) to *ground handlers*. Employees for ground handlers tend to wear a more hats, are overwhelmed, overworked, be less trained than mainline employees, and are more likely to overlook things in specific duties that a specialised employee would not miss. Look at airline targeted news for information on outsourcing at various airlines where they typically list all the stations impacted.

There is a lot of anger, resentment, and feelings of betrayal for employees of those stations. Full disclosure I ended up at a ground handler with just a handful of former mainline employees from my station. All of the union employees who decided to remain under the ground handler were called scabs and further by other union members who left for other mainline stations (unhappily).

While at my station we luckily had a few former mainline employees who ensured the transition would go fairly smoothly there were many stories about other stations where former mainline employees purposely sabotaged the new workers by destroying and removing things necessary for the operation to work.

It’s really hard to get a plane off the ground if employees cannot figure out how to order fuel, do not have the credentials to sign in nonetheless a phone number to get dispatch paperwork releases, none of the required manuals or instructions on how to do anything, get locked out of a crucial areas and don't have the phone number for the airport immediately available either because the entire flipbook of phone numbers is gone, can’t find telex printer paper…

…or can't even find where the telex printer is, and so forth.

If you have ever come across an employee who has had to move elsewhere or change to a ground handler due to this, more often than not you will hear the disdain in their voices clearly. They’ll likely openly rant about it for a while once you start them (though plenty start it themselves at the dissatisfaction rightfully so). Then they move on to the next passenger behind you.

Airline and home station loyalty truly is that strong.

Even if you ‘change’ stations your first station is forever home.

4 - INNER AIRLINE EMPLOYEE VIEWS AND ISSUES

AIRPORTITUS

Airline employees feel that they are safe and secure in their world. In addition to all of the federal fines and prison time allotted to virtually anything that occurs at the airport they also do not feel threatened by passengers, assuming that they don't know what they're doing. This condition is known as *airportitus*.

> *"The condition of a passenger immediately becoming incapable of rational or logical thinking upon entering the airport including 1337 hackers. Symptoms with this include severe irritability, anger, confusion, loss of oneself and their surrounding, crying, screaming, shouting, stop doing basic opsec. People forget things like who their airline is, go to the wrong airlines, wrong gates, leave IDs, boarding passes, wallets, laptops, tablets, phones, etc., leave them unsecured. People afflicted with airportitus are dazed out, lost their soul at the airport via TSA, the aircraft, gate areas, that type of thing."*
> *- The Avi Dictionary*

No one understands us because they're afflicted by airportitus is the mindset held by airlines. It's our own unique private world. Right?

AIRLINE EMPLOYEE VIEWS

Agents truly believe and view their world as being impossible for an outsider to understand. They don't view themselves as targets, especially if they're ticket or gate agents. They're low fish in the system outside of management and seniority, why would they get targeted?

At airline management: Don't make another dull boring online training thing they have to click through on this. Sit down with your folks. Get this into their heads: They are targets.

PASSWORDS

Over the year I worked at the airlines I chased people down regardless as to which airline they were at because of passwords.

At [airline] in the legacy system it is very easy to shoulder surf someone typing in their login as it's simply their two digit alphanumerical public sine (this is what you see on boarding passes if someone prints it for you) and four numbers. Yes, the thing preventing them from getting onto the system is literally four numbers and there's no attempt at even obfuscating the physical view of it.

Airlines should always obfuscate the entering of credentials that are supposed to be private. Not doing at least that as a bare minimum simply contradicts claims to caring about security of their employees.

Most airlines have heinous password requirements and use cases, worse if employees have to use multiple systems for different job duties. Some systems allow special characters, some cannot accept any at all, others claim a minimum of eight with special characters so employees will attempt creating passwords only to realise in the end not only are the special characters allowed limited to a very specific few but the length is capped at… eight.

Policies on the expiry of passwords vary by the airline and the systems inside of them, too. Some even require a weekly change. With no consistency across the systems it's difficult for employees to keep creating new unique passwords that fit the requirement for each system that they're on passwords usually end up like the following:

- LASDCA95 - Las Vegas to DC flight route they work, 95 for year of birth
- XXX#1229 - The three letter airline code, flight number they work on
- 4160mi#29 - The miles of a flight they work, flight number

While I'd like to remain optimistic these are real exact set ups for password creation that people have created to make it manageable and more importantly, consistent. So long as they do not run out of unique flights this setup works. Yet this still very much frustrates employees to where it is *actively encouraged amongst airline employees by management to write down their passwords*. This is highly suggested even.

Non-technical employees think it is clever to text their usernames and passwords to themselves. I have called this the password epidemic because their passwords are virtually everywhere. Their passwords and login information are on sticky notes, taped to the back of their lanyard cards, put onto their non-protected phones, typed up in emails… They are everywhere.

We have not even mentioned those frustrated enough that they hand over their credentials to other people. Or forget to logout. Sine ins or logins are persistent in many legacy systems so unless one verified that they were under their correct sine in all of their work may be done under whoever was the last to use it and not sine out.

Agents absolutely love to be clever or at least think they are. It helps with the boredom when there's nothing to do and there's no more gossip left to talk about until something else happens. Passwords happen to be one specific area of that.

Please make password requirements consistent.

USB PORTS

People absolutely love to plug in things all the time. While most of the station areas do not have physical access to USB ports especially out in the ticket counter or gates area without a key everyone who works in those areas still have access to said keys. On the other hand the office areas are essentially USB port wonderlands.

Airports clearly have a lot of lost items due to airportitus. When employees see a USB on the ground they plug it in to the dismay of a frantic Avi trying to grab the USB found from nearby a gate podium to which they smugly put it into the desktop saying, "See there's nothing wrong with it you're overreacting."

No matter what the policy is, no matter what other people tell them, people will plug things in. Sometimes it's because they really do want to help find out whose item it is but other times it's their phones, or more. Please secure those USB ports. If an employee must use a USB issue a company USB for them and restrict non-company

USBs otherwise. It’s not enough to just tell people, “Don’t plug in a USB,” stop them from being able to do it at all. The few pages of training on this isn’t enough. Prevent it from happening at all.

OLD LEGACY ENTRIES

Many airline employees, feeling as if they are in their own world separate from the rest that no one else can understand them, speak the very legacy system commands they are typing out out loud. If you pick up on the language you can figure out exactly what they are doing. This is not useful without access to a machine of course but to get an idea and pattern of their work and lingo this is an excellent place to begin.

This issue is a personal thing for employees and mostly those who know the legacy systems. Newer employees from the last two years on the other hand have essentially no exposure to the legacy systems at this point. This is great as the new systems tend to be very intuitive but also inhibit many actions that users should not have access to. On the other hand generations who’ve only known the old system now do not want to change.

Those who’ve worked with the old legacy system feel that the new systems are a burden due to the time it takes to do simple tasks. While certain tasks, such as managing the gates or doing station ops, has become much simpler with the new systems, being unable to simply rebook a passenger in a minute or less with entries as the new system takes time to load or glitches frequently, it has become a source of pain and frustration for many employees with seniority.

INSIDER THREAT

PASSIVE VS. MALICIOUS

Insider threat is a massive issue anywhere one can go, but most certainly inside of the airlines whether passively or maliciously to an airline and further.

An example of a passive issue would be the overriding of the system to give people better seats by either evading the company's logging system and/or understanding the rules to back themselves up with 'correct' documentation (against corporate policy which states you should be charging for all upgrades for revenue, etc).

This, to passengers and to a lot of employees, is a good thing. Many view the charging of seats by airlines to be ridiculous. Except if an employee can evade the logging system because they have or found a specific entry that doesn't trigger it to log there are many more possibilities in what is still accessible.

This is already being cracked down at many airlines. Yet if an employee is observant, sees what ticks the logs or not, it doesn't take much to figure out the rest. Moving people away from the raw legacy systems and only providing a standard entries guide if needed that has those entries already being logged is one way to mitigate this issue. The legacy systems are where all the access is at. Limiting entries and implementing checks and balances like [airline] did to their employees on various interactions was excellent. Also developers for the new systems may not have all of the possible entries which folks with the older entries use to evade the logging due to repeated and multiple mergers over time.

Another relatively known fact are those who take advantage of the OVS system. To briefly explain airlines purposely oversell their flights which now becomes an OVS (Over Sale/Sold) flight. Flights are OVS'd because over time with enough data they can see which flights tend to have people either miss them entirely, arrive late, and further. Due to airlines only making money if their aeroplanes have maxed out their seats by OVSing a flight you can always ensure that your flights will be full.

Statistically and on an overall this logic makes sense. In-person, however, you may wonder why every single flight feels like it's OVS'd. It may have been a miscalculation due to various things an agent may have done improperly at previous gates for it, there are a multitude of reasons. Unfortunately when a flight is a *true OVS* gate agents recognise they must find volunteers lest a passenger becomes an *invol* (involuntarily denied boarding passenger).

Anyone who is not in the airlines and has ever been 'forced' off a flight, received a flight voucher, and moved onto alternative flights may feel that they are an invol, but in fact *if they received alternative flights, they have actually accepted that they are a vol (volunteer) passenger in the system*. A *true invol* receives the cash compensation as stated lawfully but parts completely from that airline meaning they are not receiving any more flights from them, period. They must find their own way to their destination.

With the ideas of OVS flights, invol, and vol passengers set out of the way, one can easily see a few possibilities out of this. If an airline does not provide the *PBT* (Passenger Boarding Total) for employees booking NRSA flights on the employee booking system or an employee does not have access to the internet the day of flying they may call or ask the station employees to check the PBTs for them to see if it is still worth flying or waiting at the airport to non-rev. The PBT is not to be shared to the public amongst other numbers deemed sensitive as it relates to the passenger manifest. Many employees are happy to respond to one of their own and let them know what the PBT is for flights.

Setting aside social engineering possibilities out of verifying PBTs we can now enter malicious territory. If there is an insider to a specific airline not only do they get all access to the PBTs for any flight in the system across various airlines (airline A can see airline B's PBT but typically not if they are overbooked) they can start measuring over time flights that have closed and see what the outcome was. All it takes is one person to figure out the probability of a flight being an OVS flight and a true OVS then start booking passenger paid tickets in advance, whether it's attempting to be a true invol with the cash compensation or a vol with the flight vouchers.

There is also the case of employees booking themselves or others outside of the country. This would take 2-3 minutes for an average or decent typer who already knew the information necessary and how to make a fully functional reservation and print a boarding pass on [airline]. On [airline] the only requirements would be to find flight segments, grab the availability [of the seat(s) on said flight(s), get some very specific seats in which I hope that two years later they've fixed the issue], 6-7 lines total of the actual PNR information, override payment by selecting cash, enter in their APIS data, override baggage tags or use manual tags, go through security and leave the country.

Clearly this creates logs in the systems that go to several different departments but at this point an employee doing this really wouldn't care anymore. Why not use flight benefits? If the employee didn't have buddy passes and wanted to get someone out this would be one way. Or sell fake functional tickets. There's also the fact that people could possibly find a way to automate it. Plug in a USB somewhere that's open. Do tons of free flights. Make templates because they already know how to do it all. There are a lot of possibilities that are open here.

Using one’s imagination It doesn’t take much to say this is an issue.

The best thing airlines can do is remove people away from the raw legacy systems that have no restrictions. Thankfully with the new systems they have done very well with limiting access albeit with all the new security issues though they need either an all assuming list of the entries possible or limit the legacy systems, once again, to strictly using allowed entries only. In addition once again airlines must secure the USB ports. This cannot be stressed enough: stop employees from being able to plug things in, 99% of the employees do not need USB ports.

WHY ARE WE STILL USING LEGACY SYSTEMS?

Airlines use legacy reservation systems that were built in the 1970s (e.g. SABRE, SHARES). They’re all very similar with mostly syntax differences. Most of them are now going ‘in-house’ for their new systems which typically means that the backend is the legacy system with a GUI over it. Unfortunately what was created in the ‘70s is deeply rooted everywhere and now no one wants to get out of it because of the hassle, the training costs, the infrastructure overhaul, and so forth.

If someone is able to read and understand the full legacy system entries and logs it becomes very apparently and easy to read and get access to quite a lot more PII (e.g. ending credit card numbers, credit card types, on [airline] the address is there randomly at times too, etc.) than an agent needs.

As we already learned, however, everyone in the airlines knows things are constantly changing but a lot of people don’t like change. Seniority and how it works at the airline creates a toxic environment reinforcing the usage of very open systems from legacy systems to even amusing travellers with seeing a key engaged on a jetbridge in operation.

5 - FUN THINGS OBSERVED

Airlines are very aware of some prominent issues and security weak points. It’s what they do or don’t do that counts. When I was attempting to report issues of various kinds the response typically was:

“No one else would have thought of this but you.”
“Non-airline people would never understand our system.”
“It’d be a felony if someone tried to do that.”

Yet while working on my CFP and talking to friends for feedback on things I discovered or different vulnerabilities, as fun and hilarious those conversations were with them giving even more examples I may add to this eventually, a common response to most of the things I found was, "I have actually found [said issue] myself before."

LEGACY SYSTEM ERRORS

One massive complaint from anyone in the airlines are the errors with old legacy software. For example the boarding pass readers are old in terms of the software being run on them. There was a situation I observed listening to at [airline] where the gate agent was rushing to board and an unknown passenger who had not paid, aka did not have an eTicket, was able to get onto the flight without triggering the boarding pass scanner or the gate agent. That unknown passenger happened to be sitting in an exit row which only popped up on the scanner with an event notice for the exit row only as that was the most prominent event in order of relevance on the software running the gate reader. They still aren’t sure of what happened from the last time I checked as the PNR disappeared from the system.

That’s pretty scary.

A lot of glitches occur frequently in the new systems causing agents to go back into the legacy systems. Computer outage protocols are a thing but why do that when you could go into the legacy system (which can be part of the protocols themselves as a backup)? On the other hand newer employees with not much experience outside of brief training exercises do not know or retain any information on the legacy system once they get into live production with the new systems on how to use the legacy system. So there's that divide that is growing, too.

NEW SYSTEM ERRORS

On United's new system all of the errors show up fully openly on the application. You can see the exact blocks of code that caused it right there. I hadn't really delved much into web development or web vulnerability testing at the time but even I knew then that it was bizarre and not normal to have your errors be right there ruining the user experience of the app. I also hadn't realised at the time it was actually a web application, either, as employees believe it's strictly software on a computer and click on the icon to open it up.

Employees are told to ignore [the errors] or the coolest new trick to debugging it yourself, right click and hit refresh! That was the first time I realised something was strange but I had assumed the developers had created it that way on purpose so it'd be similar to using a normal browser (though the only options were refresh, copy, and paste).

It was looking at the code blocks and causing errors exactly how I ended up succeeding in getting signed in in a web browser for any machine I wanted to be on. I had not been completely sure of what the parameters were at the time until then. From the time I found the exposed URL to getting the parameters to signing in and going into restricted flights was about 10 minutes. Someone with more experience than me for sure could and likely would have done more. I still remember the feeling of going, "Holy flying macarons I'm in a restricted flight."

The other part of getting myself successfully on the system was that every single thing I needed was right there everywhere. Airlines have dutifully labelled all of the machines in a very publicly viewable way whether it be the computers, printers, and more. Surely the public can't really do anything with the machine ID because they're internal, wouldn't make sense, and they don't have access. That is if someone does not recognise what a label with some stuff on it directly attached to a monitor means and can't get their hands onto it either directly or indirectly.

What if a frequent traveller started writing all of them down? Found themselves in a browser? Signed in? No one had thought to prevent that GET request before apparently. What else have they not done yet?

If you're already inside of the system as an employee and know how to get into any restricted or locked flight the implications of consequences are even higher. In the event of a crash the airline immediately removes access to the flight and the flight manifest from the rest of the system. That way they prevent inside folks from leaking to the public and the media on who all the potential lost souls were.

But what if you can get direct access to that machine that was locked down?

Outside of that at ticket counters, gates, and so on you'll see and find phone numbers, legacy system entries for specific things, and other joyous fun things everywhere. Ask if you can use a phone sometime maybe even.

There's a label on that, too.

SOCIAL ENGINEERING

Human error occurs in every industry, in particular some of the visible and public examples of this being in the airlines. Sometimes the lack of communication causes a massive rush and fear such as when no one informs the gate agents that passengers have deplaned and are coming up the jetbridge. This causes a lot of confusion when alarms are blaring while they're working on something else at the gate and now you've got TSA fines and more looking your way. Or an inexperienced agent accidentally breaking a PNR sometimes to the point you have to redo the entire reservation.

There are also a lot of things airline employees aren't supposed to provide to the public. That includes the PBT and flight totals (total number of boarded passengers on a flight and the number of bags/cargo). They should never tell people if a specific passenger is on a flight. They're also supposed to not provide the plane off and on times along with the real-time flight movement, aircraft specific information, and more. What I mean here by on and off is:

- Out - This is when they release the brakes at the gate

- Off - This is when the aircraft is officially off the tarmac in the air
- On - This is when the wheels touch down on the tarmac landing
- In - This is when they set the brakes at the gate

Many may say, “But I can track any flight on [flight tracking site]!” That’s not fully accurate, either. Sure they may be close enough margin wise for most to be satisfied with but by the FAA and rules internationally (that all vary) the public is in a different class than the airline operating that flight. The public does not need to know the exact location of where the flight is at the given moment. Depending on where the flight is those tracking flights publicly can expect a delay of half a minute to minutes from the true flight movement location.

I am also very specific and particular of what I mean when I say ‘release the brakes’ or ‘set the brakes’ here. While I won’t go into detail here or explain more it can lead to some really fun times for passengers. In the event I am able to find a publicly searchable answer on this specific topic this will be updated with such information.

And yes, the public may have the aircraft type but every airline has their own variations of them and things they know about their aircraft that the public do not need to know.

Returning back to the human side of things there are many things that airline employees are not supposed to give out publicly. That includes once again the PBT or flight totals. They should never tell you if a specific passenger is on a flight ever…

…but airline folks are family so this happens a lot:

> *“Hi, sorry I hope I’m not bothering you but I’m trying to get back home with my family tonight plus I’ve got work tomorrow. I haven’t had any luck with flights because everyone is oversold. We’re on the standby list for another flight but is there space for [x] on this flight or are you expecting a full flight?”*

‘A few things can happen here. Either the gate agent will strictly adhere to the rules (as they should) or the agent will tell them everything. This can play out a few different ways:

> *“Can I have your itinerary?”*
> *“Did you go on [airline booking portal that shows the numbers]?”*

> *"Here let me check for you. Yup, we have [x] seats available."*
> *"We're currently booked at [x] right now, there should be seats for sure."*
> *"We're a full flight sorry."*
> *"We have plenty of seats open!"*

On the agent asking for their itinerary or about their booking numbers these are two common responses:

> *"I'm actually with [other airline] but wanted to just check here so I could switch my family over."*
> *"I'm booked with another airline right now but at this point I'm pretty desperate to get home and want to buy tickets as long as it's not oversold."*

Or maybe you're waiting in line about your delayed baggage when you hear:

> *"Hi, so I tried to non-rev my grandmother from [city] but she can't speak English, I can't contact her since her phone died, and I ended up having to buy tickets for her splitting it into two trips. I'm getting really nervous and wanted to know [if they've started boarding/if she's already onboard/when they'll be in the air/saw on Flightaware they've pushed back but don't see that it's in the air yet]."*

Once again either the agent will either follow protocol by saying they're not allowed to disclose passenger information or to look at the boards outside in the airport. Or they'll ask for an itinerary, a name, a flight, etc.

We want to be helpful to each other since it's one big family, right?

Maybe you are in line waiting to be rebooked and hear a conversation happening with someone who also works at the airlines talking to the gate agent on how to rebook them like so:

> *"Hey I know you're new to this but there's a way faster way to do this. Open up [legacy system]. Yup, there we go. Signed in? Yeah? Cool so now type this in..."*

A lot of inexperienced agents type in entries directly from airline employees even from other stations simply because they were told to do it. This is out of sheer habit from their training days and also from the help desk that they call when they run into an issue who give them pure legacy system entries to type in. There's not much people can do without access to the systems unless they can get someone else to do it for them. It's good that agents are moving away from legacy systems but until their access to it— inexperienced or experienced in it—is removed, future cases of experienced agents abusing it from mild cases of upgrading their seats to full on malicious actions will keep on occurring.

Airlines, especially in recent times, have been hit very strongly with poor PR coverage whether it be dragging paid passengers off of their aircrafts unconscious, forcing mothers to place children above two years of age on their laps for entire flights, roughly grabbing expensive violins, it's easy to get the picture that there is much work that needs to be done. They know the root of it begins at customer service and care so what are they doing to fix this?

Starting employee campaigns of course. Particularly on social media since what other way is there to raise morale than the beauty of cute photos and selfies with your coworkers? Take a look sometime at hashtags on Twitter, Facebook, Instagram, you never know what you'll see there. Employee and SIDA badges, SIDA areas, and even sensitive documents may be inadvertently snapped in these photos.

6 - CONCLUSION

While it should be no surprise that there are multitude of issues considering how human driven and focused the airlines are, the fact that they are key and core components to national and international infrastructure is extremely concerning. We are certainly fallible to making and creating mistakes as humans but due to the sheer size and nature of the workforce required to run these systems all it takes are a few disgruntled or upset, untrained or maliciously experienced agents to take it all down by accident or on purpose.

Agents are required to undergo a background check and be screened as an overall. This does not, however, stop the systematic issues and environment that has been created over the last several decades. Blind trust that the legal system will handle outliers does not stop those who become intimately familiar enough in their understanding of how the systems work together as an overall with passive or malicious intent. Moreover those with malicious intent are not concerned with the legalities of their actions or their employment once they've crossed a line.

There is also a sense of pride in one's work, thus to many employees they may not recognise that their 'passive' activities (such as overriding seats) is not truly passive at all. Well-intentioned when done for passengers in front of them as a customer service gesture, this shows the ability to abuse the system for personal gain and further. This behaviour is symptomatic to an overarching systematic problem.

We need better ways to improve and increase efficiency without compromising the security of the existing infrastructure or the livelihoods of those who work in it. Placing the burden of dealing with passengers and security on employees with threats do not solve the issue as it's a bandaid on a much larger problem that has persisted due to a toxic environment and culture that goes all the way to the top of the chain.

The airline industry provide an excellent example of how a large and seemingly unapproachable system of various companies, agencies, departments, and further, work (or do not work) together, interlocking seamlessly or clashing with one another as various players in a game on a play date. It would be in the best interest to the public and the airlines to allow researchers, including those currently or formerly involved, to be given some agency to help find and solve the issues that have persisted and exist to this day.