Development of a Cryptographically Secure Booking Reference System for Air Travels

Orimoloye Segun Michael

Department of ComputerScience,Adekunle Ajasin University,
Akungba-Akoko, Ondo State,, Nigeria

Abstract :
PNR otherwise known as Passenger Name Record in the airlines and travel industry is a record in the database of a Computer Reservation system (CRS) that consists of the passenger information for a passenger, PNR code (Booking Reference) and the itinerary for the passenger or a group of passengers travelling together. The PNR code is frequently used to enable online check-in and ticket retrievals for flights and rail travels. The coding system currently used in the travel industry by Amadeus-a foremost Global Distribution System (GDS), for PNR generation is a six (6)-character alphanumeric code comprising four (4) pseudorandom numbers, generated by the rand() function and the first two (2) characters of the passenger's first name. This coding system has been subjected to a lot of cyber-attacks such that hackers have been able to successfully guess the PNR code time and time again owing to the limitations inherent in the rand() function and overall process of the code generation. They have been able to have access to flight information of passengers, canceling flights in exchange for airline credits which they use to book new tickets, at the expense of the genuine owners of the tickets. This work therefore proposes a cryptographicallysecure booking reference system that is 8-character long with two added layer of security: an implementation specific cryptographically secure pseudorandom number and a security question/answer pair.

Keywords: *Passenger Name Record, Booking reference, Cryptography, Amadeus, Information security*

I. INTRODUCTION

The right to privacy and data protection belongs to the fundamental rights and freedom of individuals. It is also believed that effective security must be ensured in the travel industry, especially the civil aviation sector. But new surveillance and control measures being enforced, specifically the collection of air passenger personal information have a serious impact on these rights. As the result, a conflict arose between the use of personal data for security purposes and the protection of such data. When a passenger books an itinerary, the travel agent or travel website admin will automatically create a Passengers Name Record (PNR) in the Computer Reservation System (CRS), which may be the airline's database or typically one of the global distribution systems (GDSs).

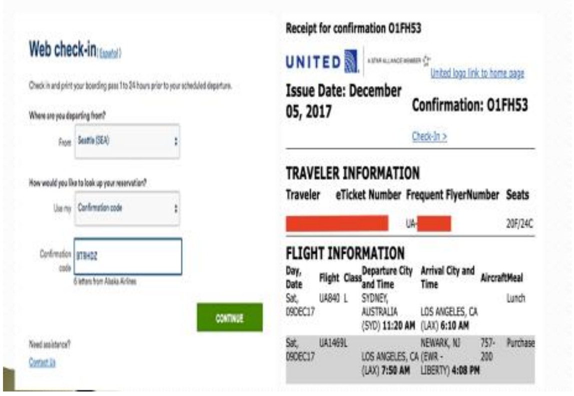
A global distribution system (GDS) is a network operated by a company that enables automated transactions between travel service providers (mainly airlines, hotels and car rental companies) and travel agencies. Travel agencies traditionally relied on GDS for services, products & rates in order to provision travel-related services to the end consumers [1]. All GDSs provide the basic functions for the reservation process such as product presentation, reservation, fare quote & ticketing and additional services. Sabre, Galileo, Amadeus, and Worldspan have emerged as the GDS's with the largest market shares [2].

A passenger name record (PNR) is a record in the database of a computer reservation system (CRS) that consists of the personal information for a passenger, booking reference (PNR code) and also contains the itinerary for the passenger, or a group of passengers travelling together [3].

A booking reference (PNR code) as an alphanumeric or alpha code, typically 6 characters in length, used in airline reservation systems to access a specific record of a passenger. This code allows for updating flight information and cancelling flights [4].

Information security experts Karsten Nohl and Nemanja Nikodijevic could access multiple records looking for bookings under the name "Smith" and using a thousand randomly generated PNR codes, five came back with active bookings, thus making the current PNR coding system seriously flawed [5].

This work is therefore aimed at developing a cryptographically secure booking references system for Air travels building upon the inadequacies of the existing system.



Web check-in (Español)

Check in and print your boarding pass 1 to 24 hours prior to your scheduled departure.

Where are you departing from?

From: Seattle (SEA)

How would you like to look up your reservation?

Use my: Confirmation code

Confirmation code: 9T8HDZ

6 letters from Alaska Airlines

CONTINUE

Need assistance?

Contact Us

Receipt for confirmation O1FH53

UNITED | A STAR ALLIANCE MEMBER

United logo link to home page

Issue Date: December 05, 2017

Confirmation: O1FH53

Check-In >

TRAVELER INFORMATION

Traveler	eTicket Number	Frequent FlyerNumber	Seats
[redacted]		UA-[redacted]	20F/24C

FLIGHT INFORMATION

Day, Date	Flight	Class	Departure City and Time	Arrival City and Time	Aircraft	Meal
Sat, 09DEC17	UA840	L	SYDNEY, AUSTRALIA (SYD) **11:20 AM**	LOS ANGELES, CA (LAX) **6:10 AM**		Lunch
Sat, 09DEC17	UA1469	L	LOS ANGELES, CA (LAX) **7:50 AM**	NEWARK, NJ (EWR - LIBERTY) **4:08 PM**	757-200	Purchase

Fig 1: Sample Flight bookings with Booking references highlighted

II. RELATED WORKS

Reference[6] proposed the establishment of cyber-security standards and best practices at U.S airports emphasizing on cyber-security education and literacy as the existing standards focus on Aircraft Control System (ACS).

Reference [7] discovered that the PNR code is weaker than a simple six-character password. They were able to come back with five active bookings by using a thousand randomly generated booking codes when looking for bookings under the name "Smith". They found out that access control was virtually non-existent allowing just anyone to access flight information of passengers when they can guess the PNR code. Reference [8] presented threat mitigation and Cyber resilience controls for smart airport Cyber-security. They carried out a risk scenario analysis of Internet of Things (IoT) malicious attacks at airport infrastructure with threat mitigation actions.

III. STATEMENT OF THE PROBLEM

Personal information of passengers have fallen into wrong hands; they have been able to cancel flights and exchange such for airline credits which they use to book new tickets at the expense of the genuine owners.

Passengers have been subjected to spam email messages by phishing attacks owing to crackers being able to guess correctly their PNR codes and thus have access to their personal information.

Unfortunately most researches on Cyber-security for the aviation sector do not focus on this. Reference [7] Nohl and Nikodijevic(2016) only talked about the problem but did not develop any framework or model for mitigation of such threats while [6] only commented on the need for the establishment of cyber-security standards in the U.S aviation industry with emphasis on cyber security education and literacy.

IV. METHODOLOGY

A. Analysis of the existing system

The current PNR coding system for booking references used by Amadeus GDS, one of the foremost GDS comprises a six-character alphanumeric code comprising two characters of the passenger's first name and four characters/numbers generated by the pseudorandom number generator function rand() with entropy provided by the seed function, srand(). The source of entropy is typically the time interval in milliseconds between the epoch in 1970 and the current system time.

rand () mod n gives a random number in the closed interval [0,n-1]

while seed function is *srand(time(NULL)).*

This has been shown to be weak.

"True" randomness can only be obtained by using an hardware random number generator which obtains its entropy (source of unpredictability) from naturally occurring events like radioactive decay and atmospheric/thermal noise but this approach is expensive and often time impractical hence the need for pseudo-randomness which gives a deterministic, uniform probability distribution.

If random numbers are generated by rand() function at 19:05 and used at 19:07, it would take an attacker approximately 120 attempts to correctly guess the sequence of numbers generated, which is the number of seconds between those times. This could even be faster with the use of bots.

B. The proposed system

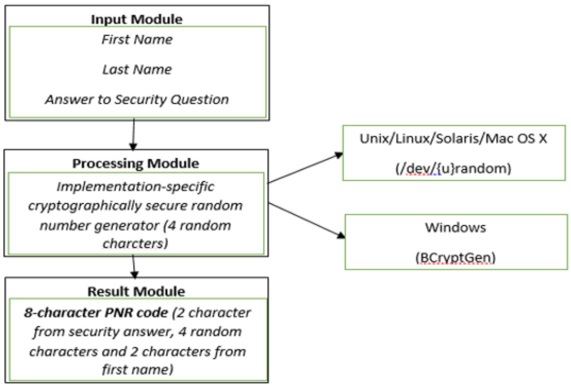

Input Module
First Name
Last Name
Answer to Security Question
Processing Module
Implementation-specific cryptographically secure random number generator (4 random charcters)
Result Module
8-character PNR code (2 character from security answer, 4 random characters and 2 characters from first name)
Unix/Linux/Solaris/Mac OS X
(/dev/(u)random)
Windows
(BCryptGen)

Fig 2: Architecture of the Proposed System

The proposed system provides a cryptographically-secure OS-specific pseudorandom set of numbers and a security question set and answerable only by the user as added layers of security.

C. Proposed system models

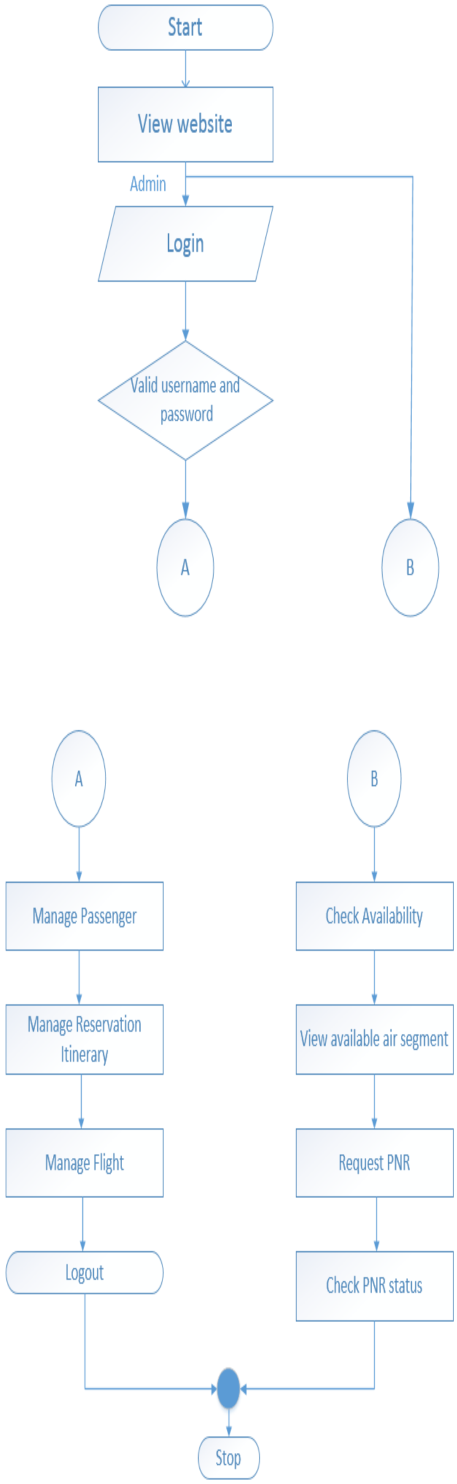


Fig 3: System FlowChart

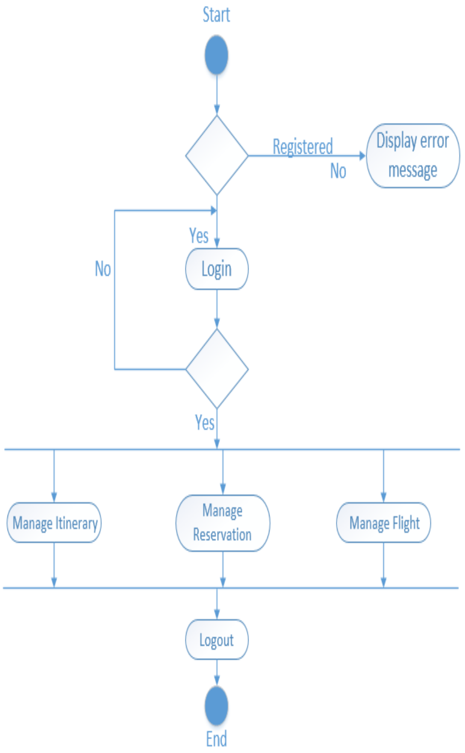


Fig 4: Activity Diagram

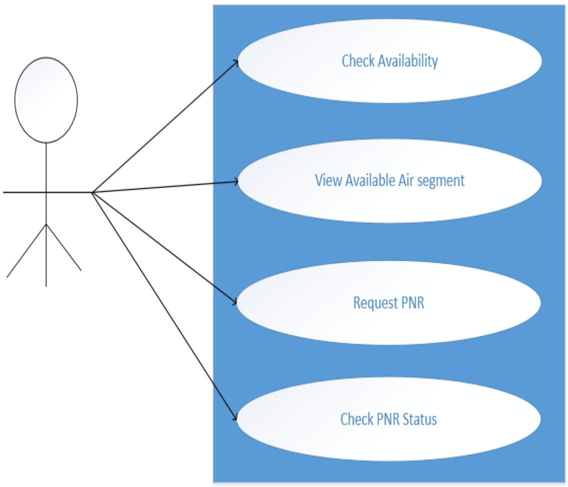


Fig 5: User/Passenger Use Case Diagram

D. Mathematical model

Let Q be the security question asked, Q ={‘a’,’b’,’c’,..z,’A’,’B’,’C’,..’Z’?’,’,’,’’..}

Security answer, A is a subset of Q, such that A C B and n(A) = 2

Let F be the First Name, F = {‘a’,’b’,’c’,..z,’A’,’B’,’C’,..,,’Z’,’’’} First Name component, FN is a subset of F such that FN C F and n(FN) = 2

Let *random* be the set of the 4 random characters obtained from the CSPRNG (/dev/{u}random or BCryptGen()) , such that it's entropy obtained from 'environmental noise' from a device driver attached to the OS is given by: $\sum_{i=1}^{n} p_i \log_2 \frac{1}{p_i}$

where p_i, p_2,….p_n are probability values in a distribution where there are n possible outcomes.

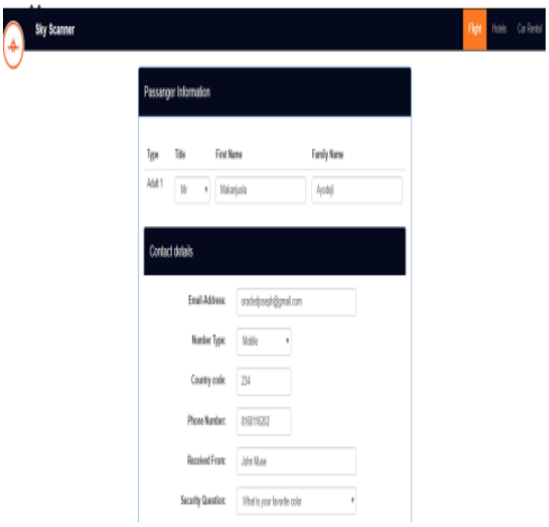
Therefore PNR code = shuffle(A U *random* U FN), the shuffle function does a re-ordering of the PNR code.

E. Pseudocode for pseudo-random number generator

```
INPUT:   (Key , Seed)

   random_data = F(Key, Seed)    // cryptographic function mapping

   Key' = F(Key, Seed +1)

   Seed' = F(Key' , Seed)

   return random_data

OUTPUT: random_data, ( Key' , 'Seed)
```

V. RESULTS

Interfaces of the prototype web application demonstrating the functionality of the proposed system are provided below:



Passanger Information

Type	Title	First Name	Family Name
Adult 1	Mr	Makanjuola	Ayodeji

Contact details

Email Address: oradedjoseph@gmail.com

Number Type: Mobile

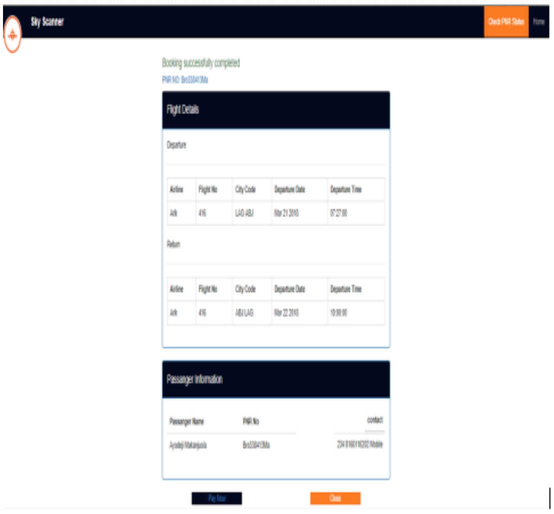
Country code: 234

Phone Number: 8160116202

Received From: John Muse

Security Question: What is your favorite color

Fig 6: Input Phase of Application



Booking successfully completed

PNR NO: Bro38413Ma

Flight Details

Departure

Airline	Flight No	City Code	Departure Date	Departure Time
Ark	416	LAG ABJ	Mar 21 2018	07:27:00

Return

Airline	Flight No	City Code	Departure Date	Departure Time
Ark	416	ABJ LAG	Mar 22 2018	10:00:00

Passanger Information

Passanger Name	PNR No	contact
Ayodeji Makanjuola	Bro38413Ma	234 8160116202 Mobile

Fig 7: Interface showing successful generation of booking reference

VI. CONCLUSION

This novel work came up with an algorithm for a new PNR coding system for the travel industry that is cryptographically secure and the random number component stands all mathematical tests for randomness- test for uniform distribution, length of period/cycle and tests of die-hardedness. A prototype web application was developed to demonstrate the functionality of the new booking reference system with hypothetical flights. Going further with this work, this new PNR coding system will be subjected to cryptanalysis to check for any vulnerabilities that could be exploited by crackers.

REFERENCES

[1] Samipatra Das (2002), 'Global Distribution Systems in Present Times' Mineola, New York City.

[2] Buhalis, D. (2003) E-tourism, 'Information Technology for Strategic Tourism Management'Gosport, UK: Prentice Hall.

[3] ICAO (2005),'International Civil Aviation Authority Facilitation Programme- API Guidelines and PNR reporting standards',Available online at https://www.icao.int

[4] Mironenko O. (2009), 'Data protection and security in civil aviation' University of Oslo

[5] The Guardian (2016), 'Airline passengers details easy prey for hackers, says researchers'. Available online at https://www.theguardian.com/technology/2016/dec28/airline-passengers-details-easy-prey-for-hackers-says-researchers

[6] Kasthurirangan Gopalakrishnan, Maniman Govindarasu, Douglas Jacobson and Brent M. Phares (2013), 'Cyersecurity for Airports', International Journal for Traffic and Transport Engineering, Vol. 3 No 4, Pages 365-376

[7] Karsten Nohl and Nemanja Nikodijevic (2016), 'Airline passengers details easy prey for hackers', Techical session at Chaos Communication Congress (33C3), Hamburg, Germany

[8] Georgia Lykou, Argiro Anagnostopoulou and Dimitris Gritzalis (2018), 'Smart Airport Cybersecurity: Threat mitigation and Cyber-resilience controls', Proceedings of the 2018 IEEE Global IoT Summit (GIoTS), Bilbao, Spain.