

Jackpotting mobile apps¹

Christian G. Papathanasiou

Disclaimer

No services or products were obtained fraudulently during the course of this research. No intention to 'permanently deprive'.

I do not represent my employer. Views and research completely my own and performed in my own personal time.

Chatham house rules.. i.e, I did not tell you any of this..

About me

Christian G. Papathanasiou

Penetration Testing Service Delivery Manager @ a UK Financial Services organization

Co-founded AthCon – the first highly technical Information Security conference in Greece

Presented at thought leading Info Sec conferences such as DEF CON & Black Hat.

MSc Info Sec / MEng Chem Eng

Interests

- Mobile App Sec
- I run a 'botnet' ☺ (of autonomous equities trading agents news / event driven strategies using kernel bypass techniques to minimise latency). Am I the only one out there?

Before we start

For those of you in here with an Android phone:

Download NeoReader from Google Play. You'll need this to scan a QR code later in this presentation 😊

App sec vulnerabilities

- Generally speaking we have become 'pretty' good at Application Security when applied to 'conventional' platforms.
 - SSDLC
 - Both manual and auto dynamic/static analysis of source code
 - Black box pentesting
 - Pre go-live and iterated upon major change
- We know where vulnerabilities lie, we know how to hunt for them..



```
<script> alert ("xss")</script>
```

Mobile App Sec vulns

- What about mobile?
 - Abstracted UI's
 - You're not meant to see the soft squidgy undercoat.
 - All pretty graphics
 - Same can be said of PC's. But you can dig under the covers with the press of a couple of buttons. Not so easy on majority of phones.
 - Various loops/hurdles iOS: jailbreak, root, cydia etc to install terminal. Android Install terminal, root devie (ROM?, priv esc in kernel?) On Linux 3.0?

Developers

In the M-World developers no longer seem to care. If it's not exposed, you can't tinker with it, why they say should it be protected?



EXCELLENT

Everything is going exactly to plan....

Common vulnerabilities seen?

- Reliance on plaintext .xml files or sqlite for storage of server-side credentials, pricing data, royalty points etc.
- Insecure storage of pricing data
- Insecure transmission of pricing data (with no retailer server side validation)
 - Retailers only get a callback from payment processor saying that payment has been approved however, no validation of was price quoted == price paid.

Jackpotting

Obtaining services or products for free as a result of manipulating application controls

We stipulate that a hypothetical international fugitive hacker needs the following basic needs for survival:

- Airfare
- Money
- Food..

We shall now examine how our hypothetical fugitive hacker would go about meeting these basic needs by exploiting mobile app vulnerabilities

Objective #1 Catch me if you can

British airways app on Android



- Upgrade from 'Blue' to 'Gold'
- Want to upgrade to 1A with no additional cost?
- Want to join priority boarding?
- Print your own boarding pass with 'Frank Abagnale' as name?
- Want to use British Airways First Class Lounge 'Concorde Room' ?

Objective #1 Catch me if you can

British airways app on Android
Upgrade from 'Blue' to 'Gold'

Just change this file:

/data/data/com.ba.mobile/files
club ID>/logindetails.xml


```
<CustomerSummary>
  <CustomerName>
    <Title>Mr</Title>
    <FirstName>Chrisitan</FirstName>
    <LastName>Papathanasiou</LastName>
  </CustomerName>
  <DateOfBirth>                </DateOfBirth>
  <PreferredEmailAddress>chris@athcon.org</PreferredEmailAddress>
  <MembershipNumber>          </MembershipNumber>
  <MembershipStatus>Active</MembershipStatus>
  <EnrolmentProgrammes>Executive Club</EnrolmentProgrammes>
  <ClubMembershipEndDate>2013-06-30+00:00</ClubMembershipEndDate>
  <AssessmentEndDate>2013-05-08+00:00</AssessmentEndDate>
  <BAMilesBalance>3614</BAMilesBalance>
  <ExecClubTier>Blue</ExecClubTier>
  <ExecClubTierPoints>20</ExecClubTierPoints>
```



3G 6:47

Executive Club details

Mr Chrisitan Papathanasiou

 Blue member
3,614 Avios points
20 Tier Points

Executive Club number:	24435015
Email:	chris@athcon.org
Membership year end:	08 May 2013
Card expiry:	30 June 2013

Objective #1 Catch me if you can

British airways app on Android

To:

```
<CustomerSummary>
  <CustomerName>
    <Title>Mr</Title>
    <FirstName>Chrisitan</FirstName>
    <LastName>Papathanasiou</LastName>
  </CustomerName>
  <DateOfBirth>1984-02-10+00:00</DateOfBirth>
  <PreferredEmailAddress>chris@athcon.org</PreferredEmailAddress>
  <MembershipNumber>24435015</MembershipNumber>
  <MembershipStatus>Active</MembershipStatus>
  <EnrolmentProgrammes>Executive Club</EnrolmentProgrammes>
  <ClubMembershipEndDate>2013-06-30+00:00</ClubMembershipEndDate>
  <AssessmentEndDate>2013-05-08+00:00</AssessmentEndDate>
  <BAMilesBalance>36140</BAMilesBalance>
  <ExecClubTier>Gold</ExecClubTier>
  <ExecClubTierPoints>20</ExecClubTierPoints>
```

As Gold:

- Priority boarding
- Use of 'Concorde Room' Lounge facilities
- Free 'Elemis Spa' massage ☺



3G 7:09

Executive Club details

Mr Chrisitan Papathanasiou

Gold member
36,140 Avios points
20 Tier Points

Executive Club number:	24435015
Email:	chris@athcon.org
Membership year end:	08 May 2013
Card expiry:	30 June 2013

Refresh Log out

Objective #1 Catch me if you can

British airways app on Android

That's great, so how do we issue a Boarding pass?

Once you perform on-line check-in, the app downloads your boarding pass as a .dat file:

Presence of .dat file == boarding pass issued.

Can create fake .dat file

File name Format:

`bp_BA0638_4GA4RE_Athens_2012-07-13.dat`

Stored in:

`/data/data/com.ba.mobile/files/24435015/bp_*`

Data is all plaintext



Objective #1 Catch me if you can

British airways app on Android

Interesting fields within boarding pass
.dat file:

flightNumber=0638

departureCityName=London

barcodeImage=base64 png array

bookingReference=4GA4RE

firstName=Christian

lastName=PAPATHANASIOU

seatRow=7

seatPosition=C

isEligibleForFastTrack=0



Objective #1 Catch me if you can

British airways app on Android

Let's completely change this boarding pass
(including bar code)

flightNumber=0638

departureCityName=London

barcodeImage=base64 png array

bookingReference=4GA4RE

firstName=Frank

lastName=Abagnale

seatRow=1

seatPosition=A

isEligibleForFastTrack=1



Objective #1 Catch me if you can

British airways app on Android

BarcodeImage is a base64 encoded PNG
Image of a non-standard Aztec barcode



GoMo News
STRATEGIC MOBILE NEWS

MOBILE ADVERTISING MOBILE BARCODES SEARCH & SOCIAL INDUSTRY PRESS

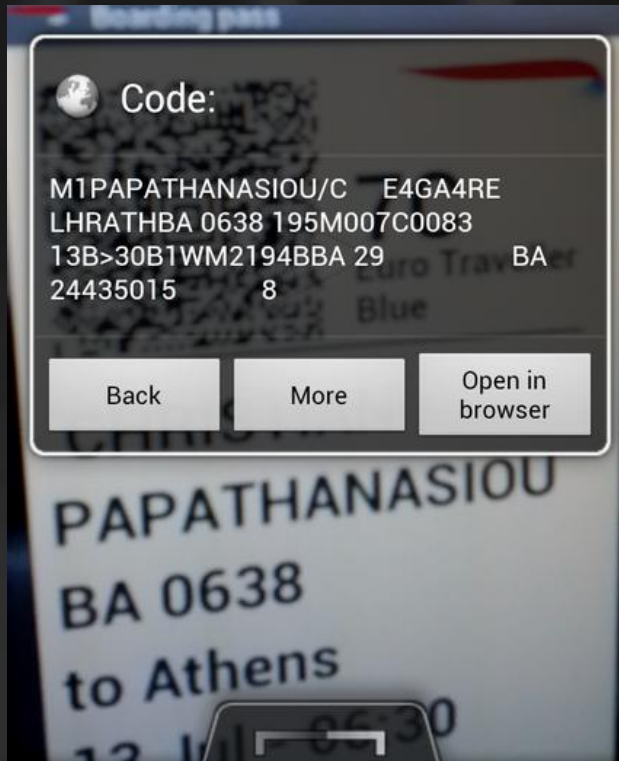
— Neustar launches Mobilenextbigthing blog India to get iPhone 4 in October

BA's barcode causes confusion – Datamatrix or Aztec?

Published on Tuesday, July 20th by Tony Dennis

Rating: Definitive proof mobile barcode world is still divided

An eagle-eyed GoMo News reader pointed out that the barcode in our recent story 'British Airways' new iPhone app uses barcodes' isn't actually a QR code as most would imagine. Reader Cameron thought BA had gone with a DataMatrix code. But actually it's an Aztec code.



Boarding pass



**Fast track
1A
Euro Traveller
Gold**

**FRANK
ABAGNALE
BA 0638
to Athens
13 Jul - 06:30**

From: **Heathrow (London)
Terminal 5**

To: Athens

Objective #1 Catch me if you can

British airways app on Android

Aztec Code Barcode Generator

 **CHAT ONLINE**
with a RACO Specialist NOW!

 **CLICK TO CALL**
and get instant answers!



Barcode Properties

```
M1ABAGNALE/F E4GA4RE LHRATHBA 0638  
195M007C0083 13B>30B1WM2194BBA 29 BA  
24435015 8
```

Code



Boarding pass



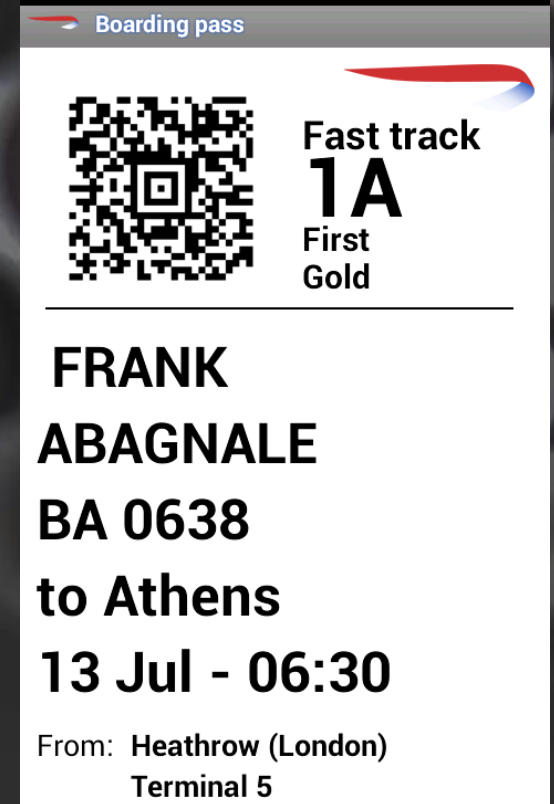
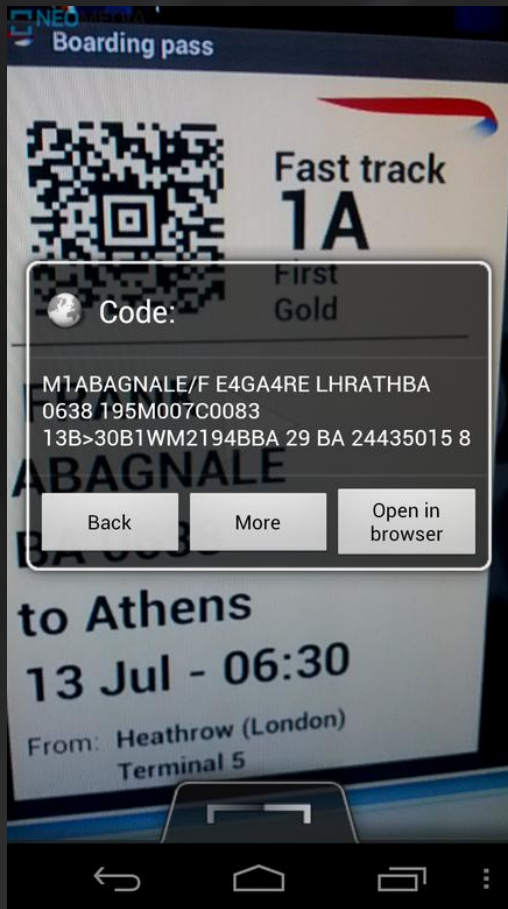
Fast track
1A
First Gold

**FRANK
ABAGNALE
BA 0638
to Athens
13 Jul - 06:30**

From: Heathrow (London)
Terminal 5

Objective #1 Catch me if you can

British airways app on Android



Objective #1 Catch me if you can

Finding idiots whose boarding pass you can spoof is 'easy'



Results for flying first class with british airways

Top people · View all

British Airways @British_Airways
Official British Airways global account. Tea... Follow

Tweets Top / All / People you follow

Royal Mail News @royalmailnews 8h
#London2012 postcode trivia quiz. Which future "Queen" of @britishswimming started out here? twitpic.com/a6pbx5
Promoted by Royal Mail News
[View photo](#)

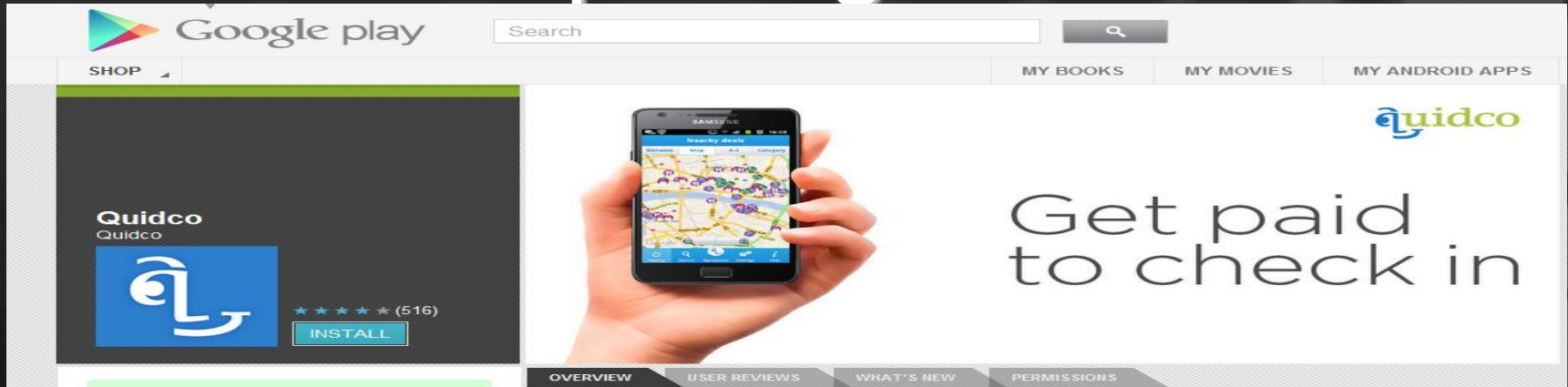
 Flying to hong kong, first class with @British_Airways - takes the edge of the fact that I'm there a mere 30 hours!
[Expand](#) [Reply](#) [Retweet](#) [Favorite](#)

You've reached the end of the Top Tweets for flying first class with british airways.
[View all Tweets.](#)

Conflict avoidance 'this is a final boarding call for..'

Can be semi automated – root app that dumps plaintext boarding pass into /data/data/com.ba.mobile/files/<exec club number>/ to speed issuing

Jackpotting Quidco



Google play Search

SHOP MY BOOKS MY MOVIES MY ANDROID APPS

Quidco

Get paid to check in

INSTALL (516)

OVERVIEW USER REVIEWS WHAT'S NEW PERMISSIONS



MailOnline

Home News U.S. | Sport | TV&Showbiz | Femail | Health | Science | Money | RightMinds |

News Home | Arts | Headlines | Pictures | Most read | News Board

The app that pays you to shop: Check-in system will offer customers rewards

By SEAN POULTER

PUBLISHED: 01:46, 4 July 2012 | UPDATED: 07:53, 4 July 2012

Comments (13) | Share | Tweet 0

Shops are to pay customers to walk through the doors under a tech revolution that could provide salvation to Britain's beleaguered high streets.

The new 'check in' system uses smart phones and GPS satellite technology to track the movements of shoppers and trigger the rewards.

The system has the support of big name retailers such as Apple, Debenhams, the Body Shop, Argos, Evans, Homebase and Carphone Warehouse.

BT Total Broadband

Quidco just announced an app that pays you to check-in to various stores across the UK. Payouts range between £0.05 to £0.50 per check-in.

Uses GPS to determine your location 😊

Jackpotting Quidco GPS Spoofing

Iran–U.S. RQ-170 incident

From Wikipedia, the free encyclopedia

On 4 December 2011, an American [Lockheed Martin RQ-170 Sentinel unmanned aerial vehicle](#) (UAV) was captured by Iranian forces near the city of [Kashmar](#) in northeastern [Iran](#). The Iranian government announced that the UAV was brought down by its Cyber warfare unit which commandeered the aircraft and safely landed it, after initial reports from Western news sources incorrectly claimed that it had been "shot down".^[1] The US government claims that the UAV malfunctioned and crashed, although the aircraft was later shown on Iranian TV with no apparent damage.^[2]

U.S. officials anonymously admitted that the drone was on a CIA spying mission over Iran when it was captured.^[3]



Iran is alleged to have used GPS Spoofing to intercept an American RQ-170 Drone. Spoof land Tehran rather than land at US Base.

If GPS spoofing can be used to bring down a drone, it surely can be used to jackpot £0.05 per check-in.

Jackpotting Quidco GPS Spoofing The hard way

- How would someone change their GPS coordinates?
- GPS device is /dev/smd27 – serial device which spews GPS NMEA data to tty
- The sys_write system call is responsible for relaying to higher layer phone functions the GPS NMEA data that is read from the GPS subsystem

Create Linux Kernel Module which:

```
if (strstr(buf, "NMEA location 1")) {  
    buf = "NMEA location 2";  
    return orig_write(fd, buf, count);  
}
```

Will always appear to be at Location2 even though at Location 1

Jackpotting Quidco GPS Spoofing The road warrior way

Fake GPS location
Lexa

★★★★★ (1,312)
INSTALL

This app is compatible with all of your devices. [+]

More from developer

OVERVIEW USER REVIEWS WHAT'S NEW PERMISSIONS

Description

Teleport your phone to any place in the world with two clicks! This app sets up fake GPS location so every other app in your phone believes you are there! Are you playing with Foursquare or with Facebook places but it's too far to drive? Find this places on the map and add them to your favorites.

Rooted users can run Fake GPS without setting "Allow mock location" option. To do that you should move "com.lexa.fakegps.apk" from "/data/app/" to "/system/app/" (use root explorer for that), set permission to rw-r-- and reboot your handset

+++ IMPORTANT +++

MORE

Nearby deals

OPEN Call store Problem? Show map

TESCO Tesco
93 Askew Road, Shepherd's Bush, London W12 9AS

Check in to earn £0.05

Offers

The Big Price Drop. Save £££ on hundreds...
Massive discounts at Tesco

Online Cashback

- 4% for Books
- 2% for Contact lenses
- 5% for Tesco Clothing

Fake GPS

Set location Stop

Map showing streets like Western Ave, Westway, Uxbridge Rd, Goldhawk Rd, King St, and Great West Rd. A yellow location pin is placed on the map.

You just checked in to Tesco and earned £0.05

3 offers nearby

- Check in and earn £0.10**
feather&black **Up to 2.3% cashback**
2.25% for all in-store sales (when purchased with any of your...
Nearest Feather & Black 0.43 miles
- Check in and earn £0.05**
orange **Get the Samsung Galaxy S3 free**
Ask in-store for details
Nearest Orange Contract 0.74 miles
- Check in and earn £0.10**
OFFICE **Futher discounts on new lines**
Save on Office Exclusives
Nearest Office Shoes 0.74 miles

Jackpotting Quidco

GPS Spoofing for mass profit

- Android Emulator has a console interface for sending 'test' events to the phone

```
ncat localhost 5554
```

```
Android Console: type 'help' for a list of commands
```

```
OK
```

```
help
```

```
Android console command help:
```

```
help|h|?      print a list of commands
```

```
geo           Geo-location commands
```

```
gsm           GSM related commands
```

```
cdma          CDMA related commands
```

```
..
```

```
try 'help <command>' for command-specific help
```

```
OK
```


Jackpotting Quidco

The mass profit way

Can fix GPS coordinate of emulator by issuing:

```
gps fix longitude latitude
```

Can get long & lat coordinates from Google Maps easily for all stores within Quidco db.

Jackpotting Quidco

The mass profit way

Create python script which
recursively sets GPS coordinates

```
import socket
import sys
s = socket.socket(socket.AF_INET, socket.SOCK_STREAM)
s.connect(('localhost', 5554))
s.sendall('geo fix %s\n' % sys.argv[1])
s.close()
```

```
for i in `cat stores`;
./geofix.py $i
./check-in.py
done
```

Jackpotting Quidco

The mass profit way

Food for thought

Application shouldn't allow you to check-in beyond closing hours. I doubt it checks for this though.

Can sleep() to account for 'travel time' checks i.e anti-superman controls – this can be polled from Google Maps (distance between point A-B)
sleep() then ./check-in.py profit.

Jackpotting Quidco The mass profit way



I can buyz

Cheezburgerz Nowz?

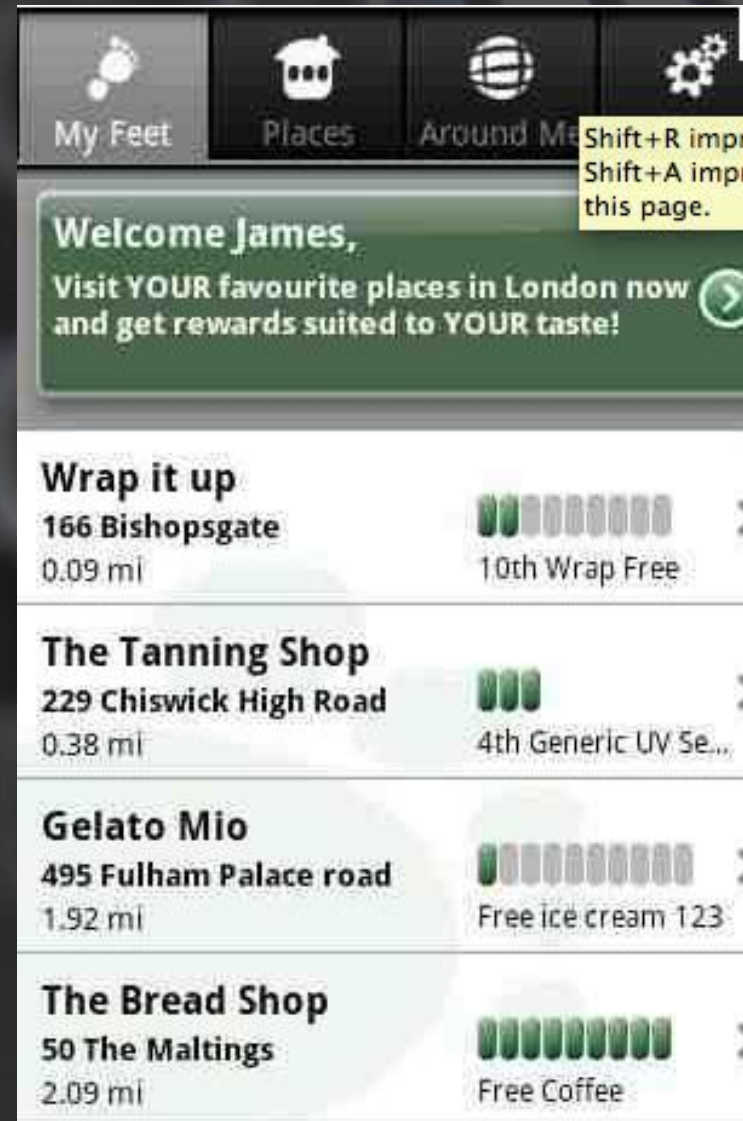
ICANHASCHEEZBURGER.COM 🐱 💰 🐱

Why find 'vulnerabilities' when you can introduce them?

Meet Stampfeet. It's a retailer royalty app.

Go to coffee house, buy coffee, present phone, employee enters 4 digit pin, app validates pin w/ server side, sends back OK, 'stamps' your royalty card.

After 4-5 stamps = free coffee, doughnut, etc



Why find 'vulnerabilities' when you can introduce them?

Food for thought:

- Decompile app dex2jar, apktool etc, add write pin to plaintext file on sdcard
- Recompile app / deploy on device
- Go back to coffee store
- Hand device to employee who enters PIN. This gets saved in plaintext file on sdcard
- Retrieve plaintext PIN, stamp own card 4 times
- Free hacker caffiene kick, doughnuts etc.

General lessons learned

Do not monitor based on GPS location. It can be easily spoofed. If you do implement compensating controls (check-ins after business hours disabled, superman detection etc)

Treat your mobile app as a thin client device. All logic and validation should rest server-side.

If static content needs to be displayed e.g, boarding pass why not .pdf and sign / verify signature of boarding pass upon opening to ensure it hasn't been tampered with on device?

OWASP Top 10 Mobile Security Controls

1. Identify and protect sensitive data on the mobile device
2. Handle password credentials securely on the device
3. Ensure sensitive data is protected in transit
4. Implement user authentication, authorization and session management correctly
5. Keep the backend APIs (services) and the platform(server) secure
6. Secure data integration with third party services and applications
7. Pay specific attention to the collection and storage of consent for the collection and use of the user's data
8. Implement controls to prevent unauthorised access to paid-for resources (wallet, SMS, phone calls, etc)
9. Ensure secure distribution/provisioning of mobile applications
10. Carefully check any runtime interpretation of code for errors

Questions?

chris@athcon.org

@ChristianPapa_

