



SISA Information Security

Global Service Centre
SISA House, 3029,
Sri Sai Darshan Marg,
13th Main, HAL II Stage,
Indiranagar, Bangalore, India.

Bluetooth Channel Penetration Test Report

ALHAMRANI UNIVERSAL



FIME®

One Action. A billion transactions.

CONFIDENTIAL

BLUETOOTH CHANNEL PENETRATION TEST REPORT

We are pleased to announce that we have completed the **Bluetooth Channel Penetration Test** for **ALHAMRANI UNIVERSAL**. We have enclosed the detailed findings and recommendations.

We value the opportunity to work with you and appreciate the cooperation provided to us during the penetration testing activity. We would be pleased to discuss any further clarifications with respect to the report and please feel free to revert to us.

Yours sincerely,

Technical Security Services

SISA Information Security

CONFIDENTIAL

Table of Contents

1. REPORT SUMMARY 4

1.1 Scope of the Penetration Test 5

2. EXECUTIVE SUMMARY 6

2.1 Introduction..... 6

2.2 Vulnerability Level Classification 7

2.3 Overall Findings..... 8

2.4 Graphical Summary of Findings 9

3. FINDINGS SUMMARY 10

4. TEST DETAILS 11

4.1 Unencrypted Data Transmission 11

5. RISK RATING 13

6. APPENDIX 14

6.1 Test Approach..... 14

CONFIDENTIAL

1. Report Summary

Title	Bluetooth Channel Penetration Test Report
Date	June 2018
Version History	Application Penetration Test Report v1.1
Author	SISA Information Security

CONFIDENTIAL

1.1 Scope of the Penetration Test

Organization	ALHAMRANI UNIVERSAL
Time Frame	6 th April 2018 – 29 th June 2018
Application/IP Tested	Bluetooth Channel
Device	MPOS – Ingenico Link/2500

CONFIDENTIAL

2. Executive Summary

2.1 Introduction

SISA Information Security, an Information security specialist firm conducted the **Bluetooth Channel Penetration Test** for **ALHAMRANI UNIVERSAL**. The penetration test was conducted with the tools and techniques that the malicious hacker uses to compromise the information with respect to Confidentiality, Integrity and Availability of the application.

The aim of the penetration test (pen test), also called ethical hacking, is to simulate an attack on the Mobile application to uncover all security issues of the application and of the data stored by it. By doing a controlled simulation of an attack, a penetration test uncovers security flaws in a realistic way. The attacking methods are also varied and range from passive scanning to targeted automated and manual attacks to exploit a specific vulnerability.

The penetration test was conducted by SISA consultants from **6th April 2018 – 20th April 2018**. The revalidation to confirm the closure of reported issues was conducted on **29th June 2018**.

2.2 Vulnerability Level Classification

Individual Vulnerability Rating – It should be noted that the overall business risk caused by any of the issues found is outside our scope. This means that some risk reported as high from a technical perspective may be considered as medium, low or acceptable, as a result of other compensating controls unknown to us. Individual vulnerability should calculate on the basis of three properties.

- Impact on the business** How the business will be affected if that particular vulnerability is exploited.
- Ease of exploitation** Skill level required to exploit the vulnerability like skilled, moderate or script kiddies.
- Exposure** What is the exposure of application for example it is available for public user, registered user or only internal users.

Risk Level	Description
High	High Risk vulnerability can be exploited by an intruder to get full administrative access to the application or its primary operating system.
Medium	Medium Risk vulnerability discloses information about the application and its underlying communications that can be used by an attacker in conjunction with another vulnerability to gain administrative power on the application or its primary operating system.
Low	Low Risk vulnerability can result in inventory of vital information held by or about the application or its primary operating system.

2.3 Overall Findings

SISA has covered all possible tests, initiated from the automated tools, and finished with manual testing and exploitation attempts. The overall assessment summary is as below:

Number of Applications/URLs Tested	1
Total Number of Vulnerabilities Discovered	1
High Severity	1
Medium Severity	0
Low Severity	0
Informational	0

2.4 Graphical Summary of Findings



3. Findings Summary

Sr. No.	Vulnerability Name	Affected Platform	Severity Level	Result
1.	Unencrypted Data Transmission	Bluetooth Channel	High	CLOSED

CONFIDENTIAL

4. Test Details

4.1 Unencrypted Data Transmission

In order to secure data that is being transferred, TLS/SSL makes use of one or more cipher suites. Transmission of data in plain text is vulnerable to eavesdropping and Man In the Middle attack, resulting in the sniffing of sensitive data.

Proof of Concept:

The image shows a Wireshark network traffic capture. The display filter is set to 'Packet bytes' and the search string is '55551234'. The packet list pane shows several Bluetooth HCI ACL packets. Packet 5270 is expanded to show the raw data bytes, with the sequence '55551234' highlighted in yellow, indicating the captured unencrypted data.

No.	Time	Source	Destination	Protocol	Length	Info
5261	11839.388987	localhost ()	Ingenico_f9:c2:8a ()	RFCOMM	59	Sent UIH Channel=7
5262	11839.389481	controller	host	HCI_EVT	7	Rcvd Command Status (Exit Sniff Mode)
5263	11839.523212	controller	host	HCI_EVT	8	Rcvd Number of Completed Packets
5264	11839.523362	controller	host	HCI_EVT	9	Rcvd Mode Change
5265	11841.149919	Ingenico_f9:c2:8a ()	localhost ()	RFCOMM	14	Rcvd UIH Channel=7 UID
5266	11844.530790	host	controller	HCI_CMD	14	Sent Sniff Mode
5267	11844.534336	controller	host	HCI_EVT	7	Rcvd Command Status (Sniff Mode)
5268	11844.537138	controller	host	HCI_EVT	9	Rcvd Mode Change
5269	11851.137500	host	controller	HCI_CMD	6	Sent Exit Sniff Mode
5270	11851.139783	localhost ()	Ingenico_f9:c2:8a ()	RFCOMM	186	Sent UIH Channel=7

```

0000  02 0b 20 b5 00 b1 00 80 01 3b ef 58 01 7e 21 45  . . . . . ;.X~!E
0010  00 00 a7 00 4f 00 00 fe 06 b7 fd 01 01 01 01 01  . . . . . 0 . . . . .
0020  01 01 02 c0 03 14 44 6c dd cc 02 44 a4 8d f1 50  . . . . . 01 . . . . . D . . . . . P
0030  18 40 00 02 a5 00 00 79 00 00 00 00 01 00 01 00  . @ . . . . . y . . . . .
0040  00 81 00 00 01 60 00 00 00 00 82 81 01 20 00 40  . . . . . . . . . . @
0050  08 00 00 00 30 30 30 30 31 33 31 33 81 02 20 00  . . . . . 0000 1313 . .
0060  40 01 00 00 00 31 81 03 20 00 40 01 00 00 00 30  @ . . . . . 1 . . @ . . . . 0
0070  81 07 20 00 40 01 00 00 00 31 81 09 20 00 40 31  . . @ . . . . 1 . . @ 1
0080  00 00 00 02 50 55 52 31 32 33 1c 31 32 33 34 35  . . . . . PUR1 23.12345
0090  36 37 38 39 30 1c 30 30 30 30 30 30 30 31 33  67890.00 00000013
00a0  31 33 1c 1c 1c 32 30 35 35 35 35 31 32 33 34  13 . . . . . 20 55551234
00b0  35 1c 03 4a 83 ff 76 7e a5  . . . . . 5 . . J . . vv ~ .
    
```

Recommendation:

Encryption must be enabled for the Bluetooth data communication.

BLUETOOTH CHANNEL PENETRATION TEST REPORT

Proof of Concept after Fix:

No.	Time	Source	Destination	Protocol	Length	Info
335	19.158908	controller	host	HCI_EVT	8	Rcvd Number of Completed Packets
336	19.185655	Ingenico_f9:c2:8a (...)	04:d1:3a:85:ab:88 (...)	RFCOMM	14	Rcvd UIH Channel=7 UID
337	19.677816	Ingenico_f9:c2:8a (...)	04:d1:3a:85:ab:88 (...)	RFCOMM	14	Rcvd UIH Channel=7 UID
338	20.198641	04:d1:3a:85:ab:88 (...)	Ingenico_f9:c2:8a (...)	RFCOMM	19	Sent UIH Channel=7
339	20.202656	controller	host	HCI_EVT	8	Rcvd Number of Completed Packets
340	20.229717	Ingenico_f9:c2:8a (...)	04:d1:3a:85:ab:88 (...)	RFCOMM	26	Rcvd UIH Channel=7 UID
341	20.483152	04:d1:3a:85:ab:88 (...)	Ingenico_f9:c2:8a (...)	RFCOMM	54	Sent UIH Channel=7 UID
342	20.487586	controller	host	HCI_EVT	8	Rcvd Number of Completed Packets
343	20.514558	Ingenico_f9:c2:8a (...)	04:d1:3a:85:ab:88 (...)	RFCOMM	50	Rcvd UIH Channel=7 UID

▶ Frame 339: 8 bytes on wire (64 bits), 8 bytes captured (64 bits)
▶ Bluetooth
▶ Bluetooth HCI H4
▶ Bluetooth HCI Event - Number of Completed Packets

0000 04 13 05 01 02 00 01 00

Packets: 1243 · Displayed: 1243 (100.0%) · Load time: 0:0.38 | Profile: Default

Conclusion:

After fix, user data is transmitted using secure encrypted channel to avoid sniffing of the data.

5. Risk Rating

The Technical Security Services team at SISA Information Security has performed the **Bluetooth Channel Penetration Test** for **ALHAMRANI UNIVERSAL**.

The overall current security posture of the application is **GOOD**.

Yours truly,

Technical Security Services

SISA Information Security

Date: 29th June 2018

CONFIDENTIAL

6. Appendix

6.1 Test Approach

Bluetooth Penetration Test is an attack simulation that is intended to expose the effectiveness of an application's security controls by highlighting risks posed by actual exploitable vulnerabilities. The testing model is built around a manual testing process. This process is intended to go much further than the generic responses, false positive findings, and lack of depth provided by automated application assessment tools.

CONFIDENTIAL