教育部資訊安全人才培育計畫

110年度新型態資安暑期課程

Advanced Information Security Summer School

Hacking OT By Bluetooth Attack

C3-1 林天佑
C3-2 楊冠彥
C3-3 劉定睿
C3-4 劉一呈

Wireless Communication Attack

- Eavesdropping
- Masquerade
- Denial of Service (DOS)
- Man-in-the-middle Attack

What Protocol Can Hacker Do Wireless Communication Attack

- WIFI
- **Bluetooth**
- Zigbee/Z-wave
- Sigfox
- another Proprietary protocol

Bluetooth Attack

- BlueSmacking
- BlueJacking
- BlueSnarfing
- BlueBugging

What May Attackers Thinking? And The Risk Of OT?

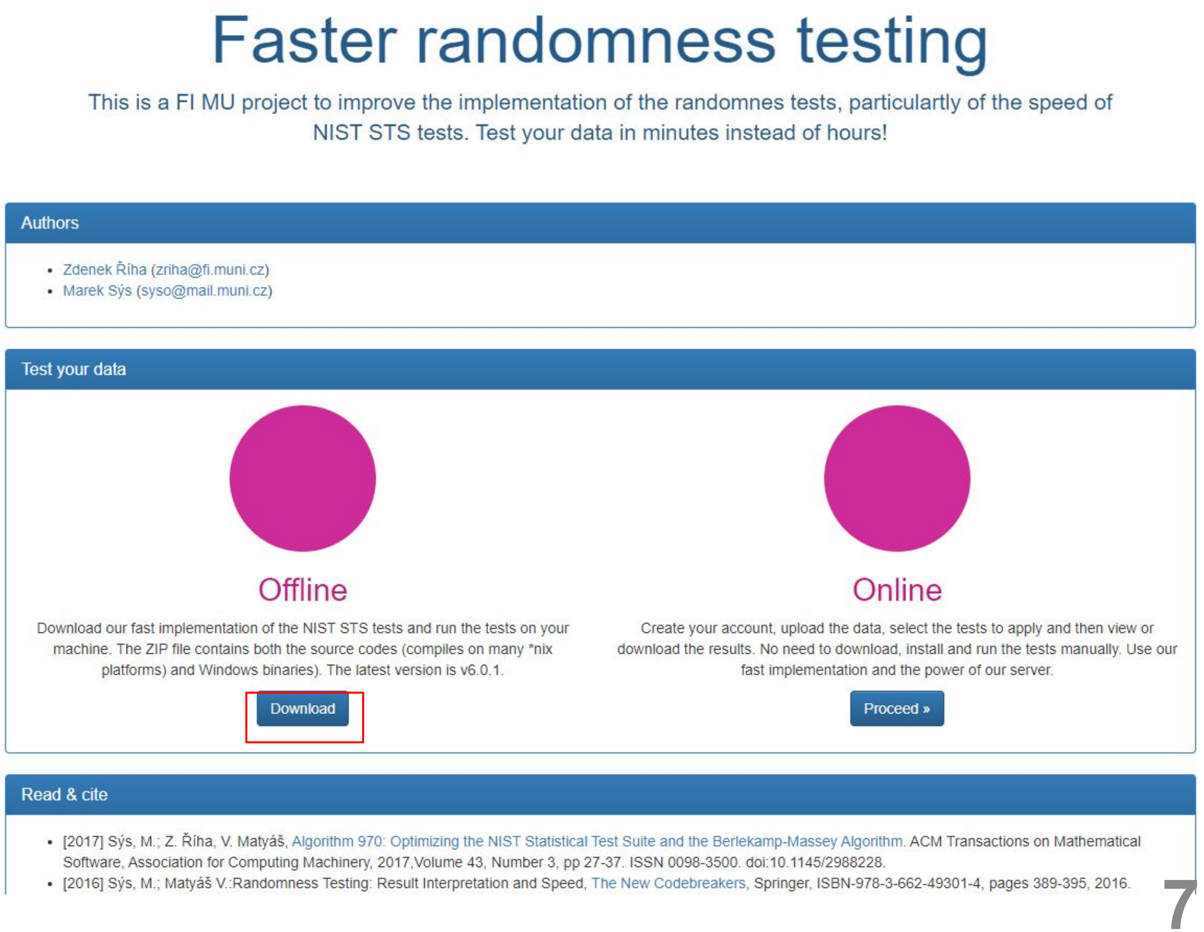
- Attackers can intercept the sensitive information that operators didn’t encrypt. Including authentication material passed over the network.
- Attackers can also use the sensitive information which intercept by MIMA. And then start another attack, Including APT, Malware attack or break the HMI/PLC.

DEMO

Tools Preparing For Testing Bluetooth Security

- Hardware
  1. Ubertooth One
  2. Raspberry Pi

- Software
  1. Eclipse3.8 / Nginx / Mariadb / Python3 / Tomcat8 / Java8 / GNU C++ / Wireshark 2.2
  2. Statistical Test Suite
     - http://frt.fi.muni.cz/



Faster randomness testing

This is a FI MU project to improve the implementation of the randomnes tests, particularly of the speed of NIST STS tests. Test your data in minutes instead of hours!

Authors

- Zdenek Říha (zriha@fi.muni.cz)
- Marek Sýs (syso@mail.muni.cz)

Test your data

Offline

Download our fast implementation of the NIST STS tests and run the tests on your machine. The ZIP file contains both the source codes (compiles on many *nix platforms) and Windows binaries). The latest version is v6.0.1.

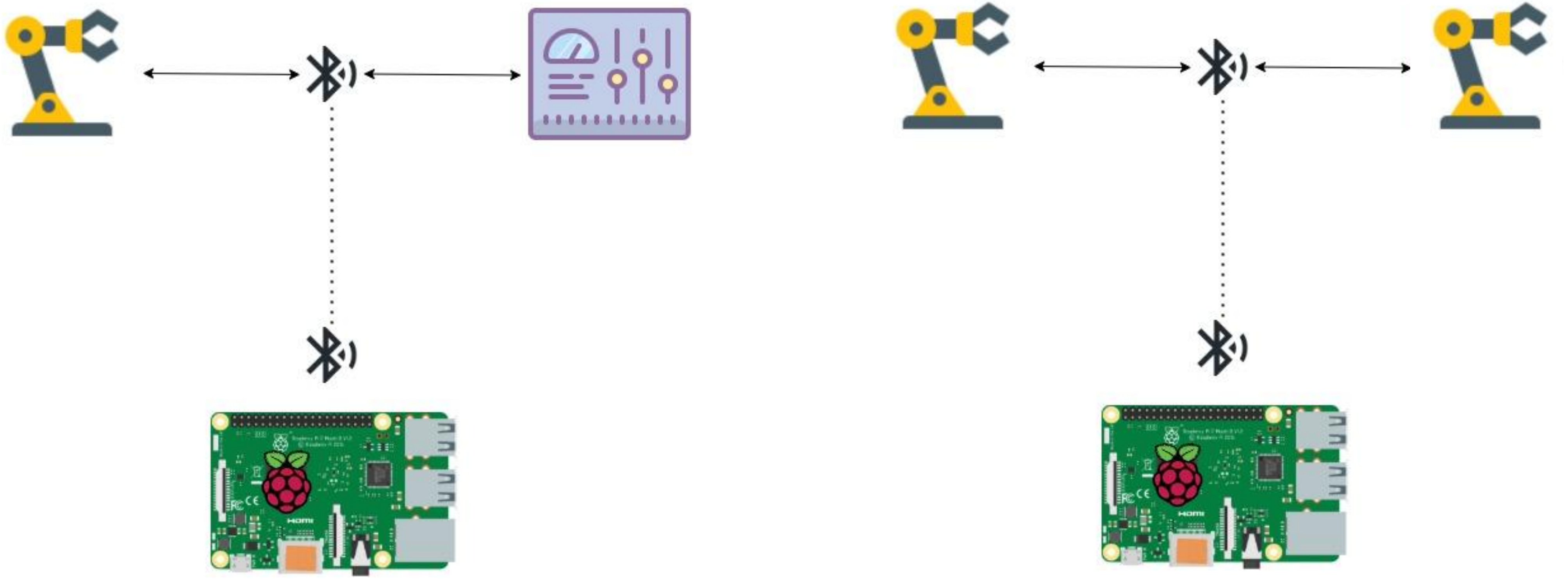
Online

Create your account, upload the data, select the tests to apply and then view or download the results. No need to download, install and run the tests manually. Use our fast implementation and the power of our server.

Read & cite

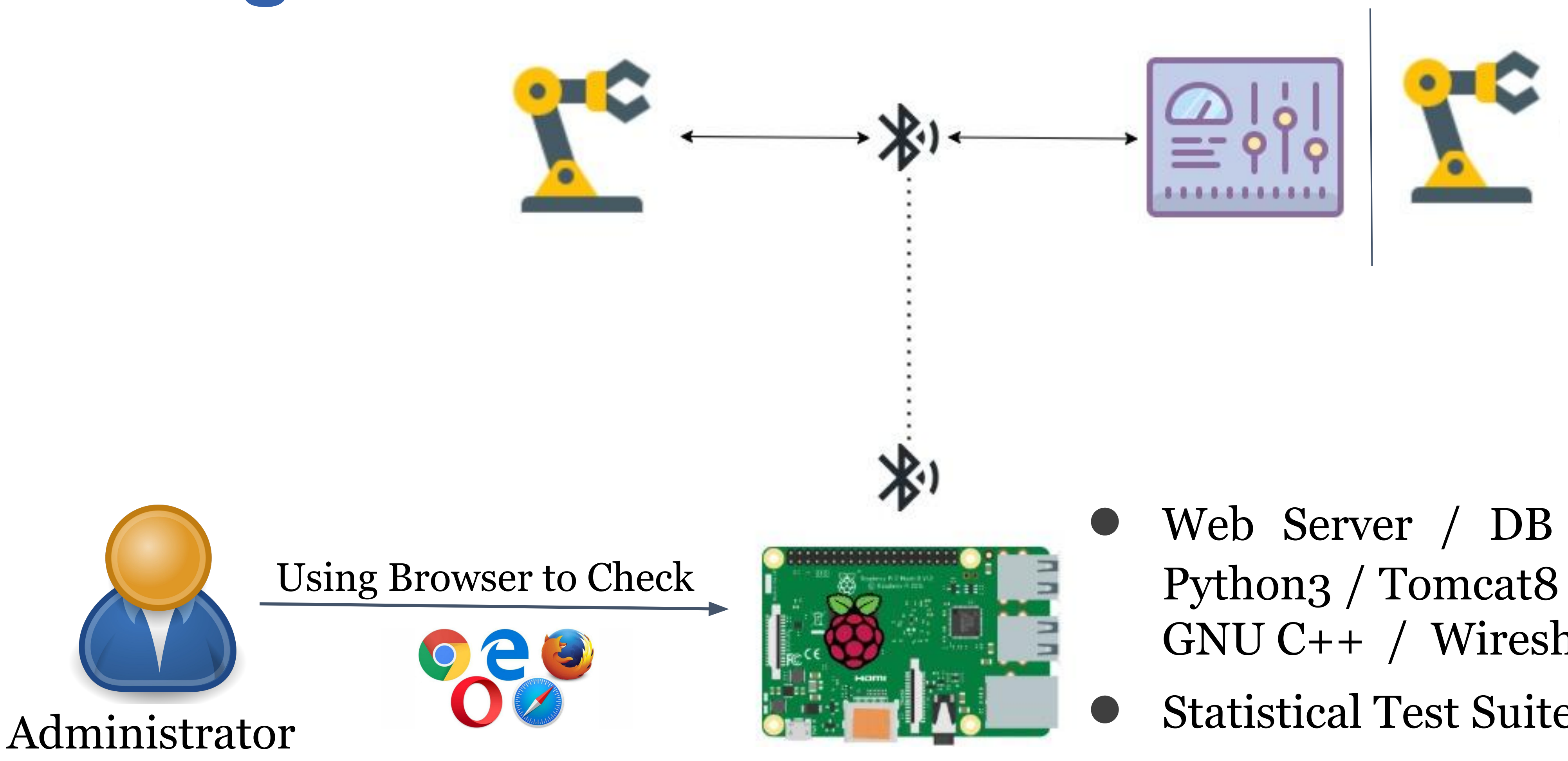
- [2017] Sýs, M.; Z. Říha, V. Matyáš, Algorithm 970: Optimizing the NIST Statistical Test Suite and the Berlekamp-Massey Algorithm. ACM Transactions on Mathematical Software, Association for Computing Machinery, 2017,Volume 43, Number 3, pp 27-37. ISSN 0098-3500. doi:10.1145/2988228.
- [2016] Sýs, M.; Matyáš V.:Randomness Testing: Result Interpretation and Speed, The New Codebreakers, Springer, ISBN-978-3-662-49301-4, pages 389-395, 2016.

Testing Environment



Icons by icon8

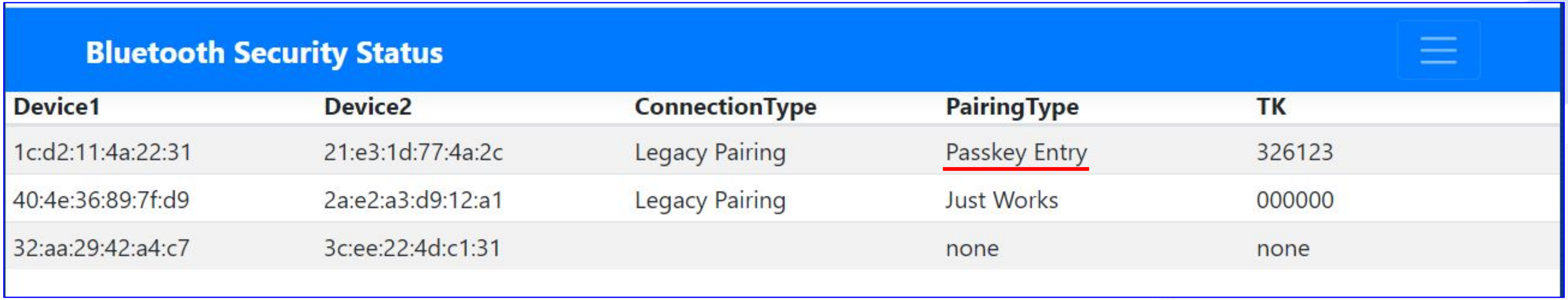
Testing Environment



- Web Server / DB Server / Python3 / Tomcat8 / Java8 / GNU C++ / Wireshark 2.2
- Statistical Test Suite (STS)

Icons by icon8

Bluetooth Security Status Inspection



Bluetooth Security Status

Device1	Device2	ConnectionType	PairingType	TK
1c:d2:11:4a:22:31	21:e3:1d:77:4a:2c	Legacy Pairing	Passkey Entry	326123
40:4e:36:89:7f:d9	2a:e2:a3:d9:12:a1	Legacy Pairing	Just Works	000000
32:aa:29:42:a4:c7	3c:ee:22:4d:c1:31		none	none

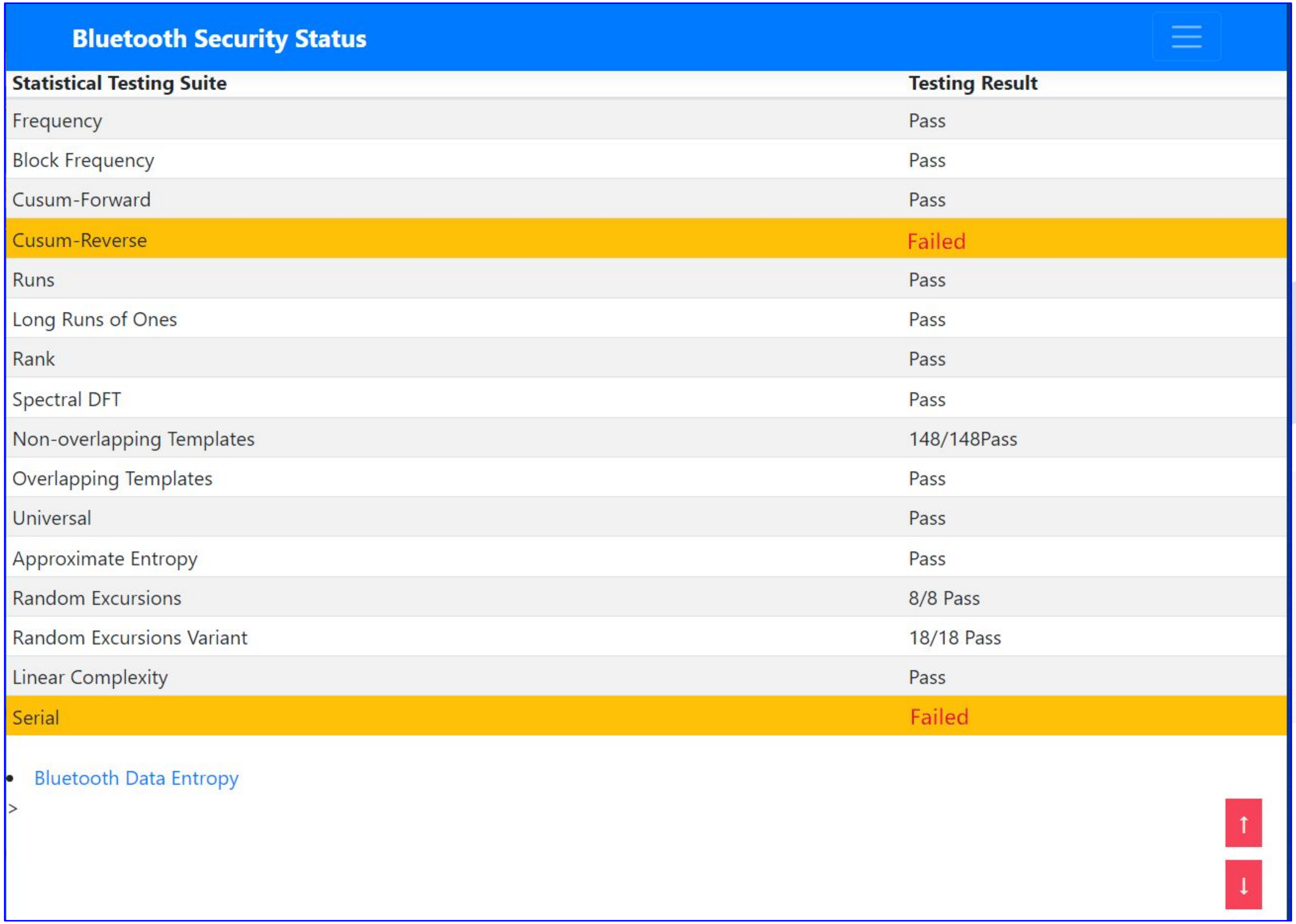
Passkey Entry: The user is shown a six-digit number 326123 on the device with a display and then asked to enter the number on the other device. If the number entered in the other device is correct, the connection is paired.

Just Works: The Temporary Key value that devices exchange during the second phase of pairing is set to 0, and devices generate the Short Term Key value based on that.

Situation A

Two Tests is fail.

Good Result!



Bluetooth Security Status

Statistical Testing Suite	Testing Result
Frequency	Pass
Block Frequency	Pass
Cusum-Forward	Pass
Cusum-Reverse	Failed
Runs	Pass
Long Runs of Ones	Pass
Rank	Pass
Spectral DFT	Pass
Non-overlapping Templates	148/148Pass
Overlapping Templates	Pass
Universal	Pass
Approximate Entropy	Pass
Random Excursions	8/8 Pass
Random Excursions Variant	18/18 Pass
Linear Complexity	Pass
Serial	Failed

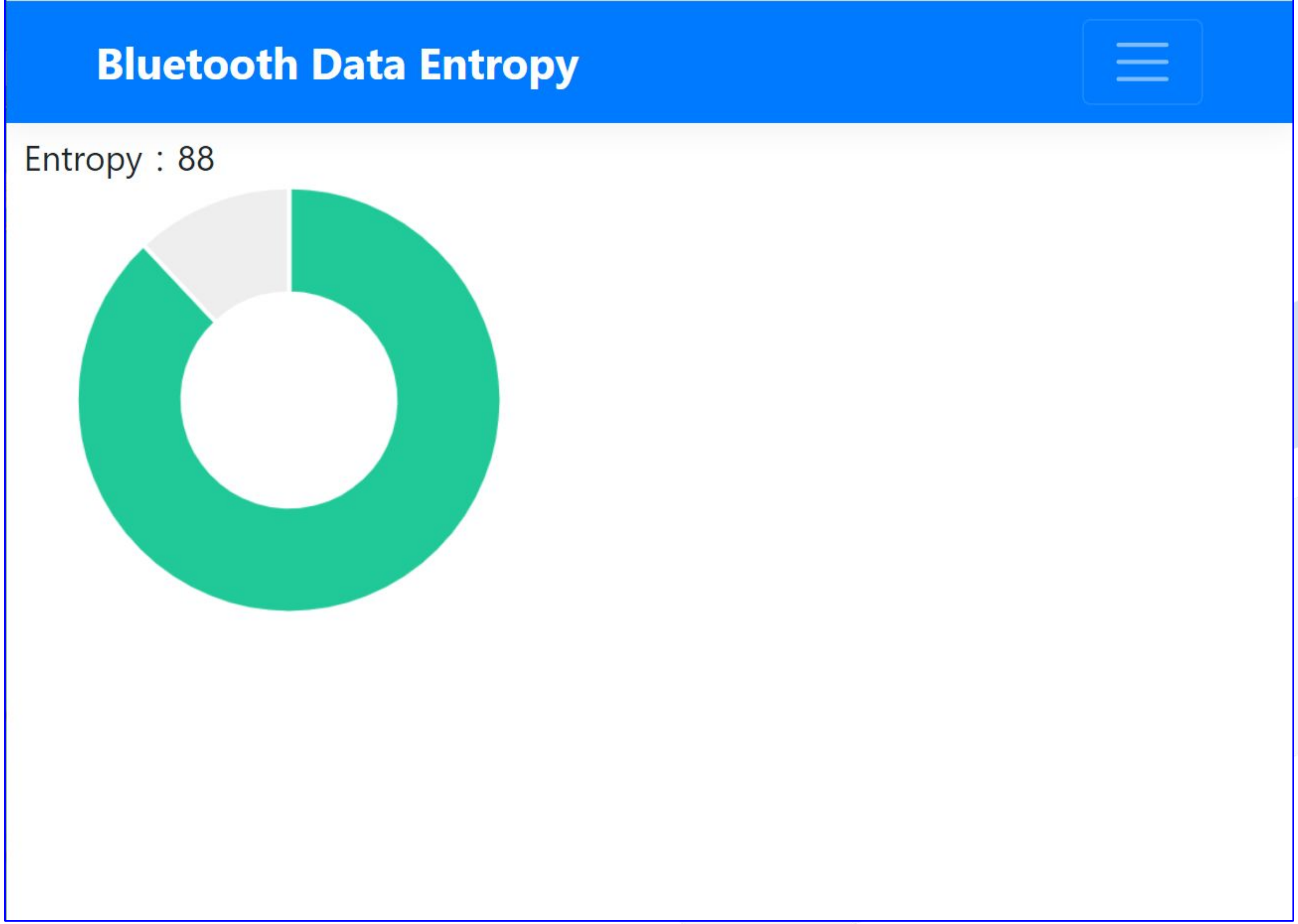
- Bluetooth Data Entropy

>

Situation A

Entropy: 88

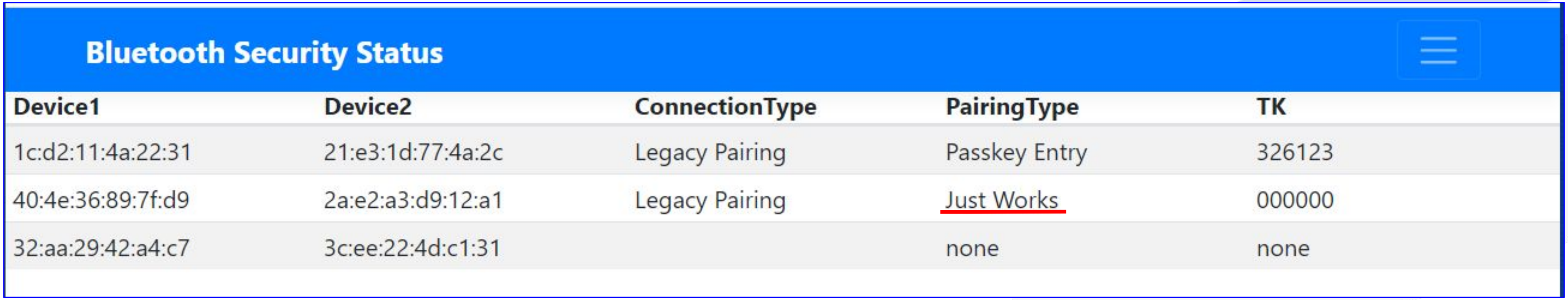
Good Result!



Bluetooth Data Entropy

Entropy：88

Bluetooth Security Status Inspection



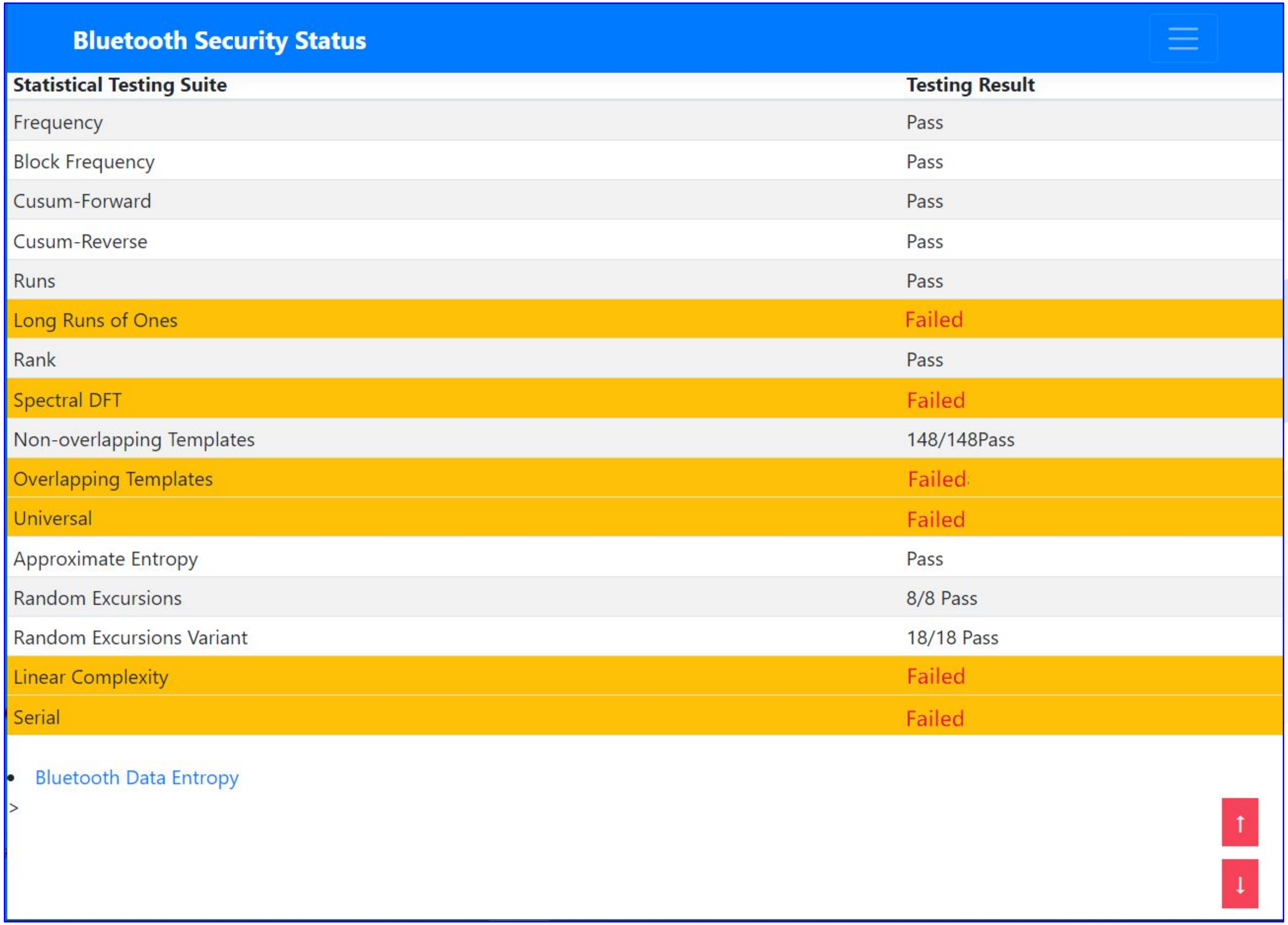
Bluetooth Security Status

Device1	Device2	ConnectionType	PairingType	TK
1c:d2:11:4a:22:31	21:e3:1d:77:4a:2c	Legacy Pairing	Passkey Entry	326123
40:4e:36:89:7f:d9	2a:e2:a3:d9:12:a1	Legacy Pairing	Just Works	000000
32:aa:29:42:a4:c7	3c:ee:22:4d:c1:31		none	none

Situation B

Six Tests is fail.

Not Good!



Bluetooth Security Status

Statistical Testing Suite	Testing Result
Frequency	Pass
Block Frequency	Pass
Cusum-Forward	Pass
Cusum-Reverse	Pass
Runs	Pass
Long Runs of Ones	Failed
Rank	Pass
Spectral DFT	Failed
Non-overlapping Templates	148/148Pass
Overlapping Templates	Failed
Universal	Failed
Approximate Entropy	Pass
Random Excursions	8/8 Pass
Random Excursions Variant	18/18 Pass
Linear Complexity	Failed
Serial	Failed

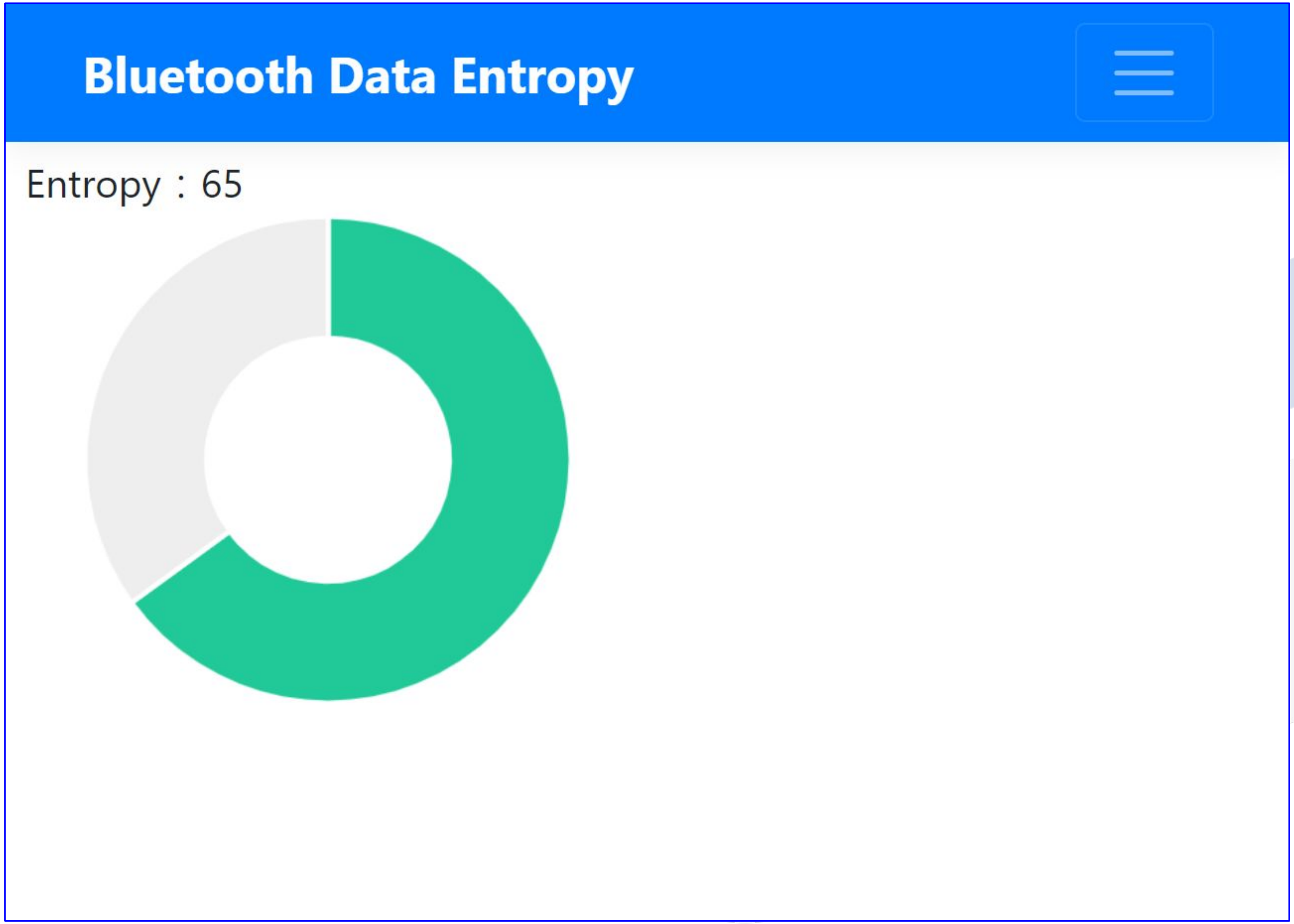
- Bluetooth Data Entropy

>

Situation B

Entropy: 65

Not Good!



Bluetooth Data Entropy

Entropy：65

Conclusion

Reference

- https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-22r1a.pdf
- https://www.cc.ntu.edu.tw/chinese/epaper/0003/20071220_3006.htm
- https://secbuzzer.co/post/22
- https://cybersecurity.att.com/blogs/security-essentials/bluetooth-security-risks-explained
- https://attack.mitre.org/techniques/T1040/
- https://ithelp.ithome.com.tw/articles/10223483

Thanks for listening

Q&A