

Vulnerability Analysis and Mitigation of MIL-STD-1553 Communication Protocol

Gavin Blankenship, Appalachian State University
Weichao Wang, College of Computing and Informatics



Introduction

MIL-STD-1553 is a widely-used network protocol that was published by the United States Department of Defense in 1975. It was created for military avionics. The protocol is currently being used for many military and civilian applications because of its flexibility and easy adoption.

For many years this protocol has been reasonably secure from attacks because of its physical isolation from the external world. Due to technological advances in connectivity, it has become a priority that operators/pilots can detect and protect the subsystems within an aircraft using MIL-STD-1553.

Objectives

- Learn the history and details of MIL-STD-1553 and explore each part of the protocol, along with its function.
- Use/create a working simulation of the protocol and track the packets being sent to and from the classes in the simulation.
- Investigate potential attacks on the simulator to expose vulnerabilities within the protocol.
- Create ways to detect and protect the protocol using the information found during the attacks.
- Map the protocol and its vulnerabilities to other legacy protocols for future investigations.

Method

Programming Language

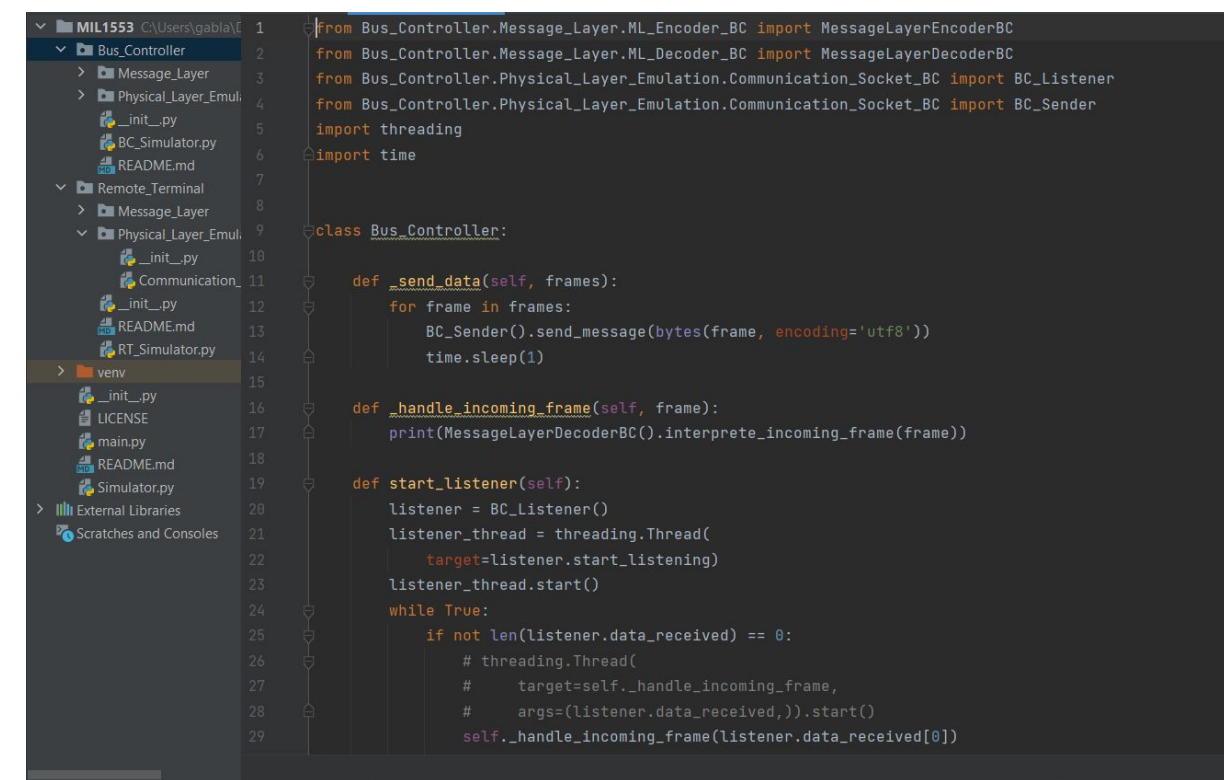
Python version 3.9.

IDE

PyCharm

Simulation Code

- The simulation code was acquired from GitHub and was thoroughly analyzed before using. The code was created by Shubhankar Kulkarni.



Related Work

Cybersecurity on Avionics (AIM)

- The company AIM has developed a suite of tools that will help analyze, attack, detect, and remove potential security vulnerabilities. Some security concerns were found considering that the data bus is an interaction of many subsystems.

Exploiting the MIL-STD-1553 (Science Direct)

- The multiplexing and scheduling scheme causes a single point of failure
- Attackers could learn the frame scheduling and execute malicious actions during convenient bus times.

Results

- During research, I have found that there are many vulnerabilities within MIL-STD-1553.
- Several papers I have read indicate that MIL-STD-1553 has little to no defense mechanisms against cyber attacks. Many also suggest that the protocol will have to detect an attack before it can protect it.
- We have found that the messages sent to and from other classes in the simulator are very simple. Which makes it easy for attackers to compromise the system. There is also no authentication measures in place.

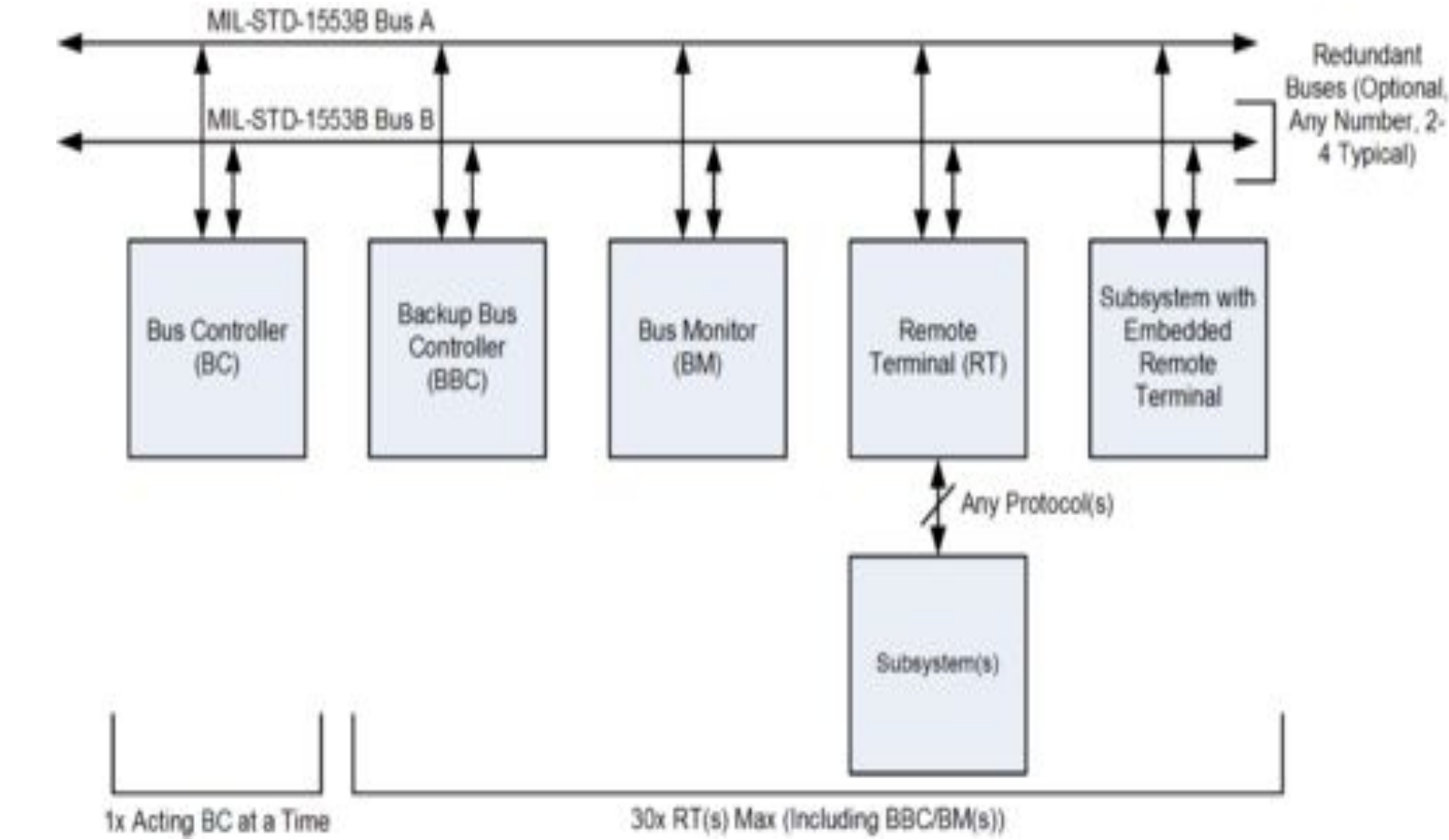


Diagram of MIL-STD-1553

No.	Time	Source	Destination	Protocol	Length	Info
8	36.530218	192.168.1.9	255.255.255.255	UDP	62	58915 → 2002 Len=20
9	37.530693	192.168.1.9	255.255.255.255	UDP	62	58916 → 2002 Len=20
10	38.530317	192.168.1.9	255.255.255.255	UDP	62	58917 → 2002 Len=20
11	39.566605	192.168.1.9	255.255.255.255	UDP	62	58918 → 2002 Len=20
13	40.575853	192.168.1.9	255.255.255.255	UDP	62	58919 → 2002 Len=20
15	41.585016	192.168.1.9	255.255.255.255	UDP	62	58920 → 2002 Len=20
17	42.589145	192.168.1.9	255.255.255.255	UDP	62	58921 → 2002 Len=20
19	43.600553	192.168.1.9	255.255.255.255	UDP	62	58922 → 2002 Len=20
24	64.542229	192.168.1.9	224.0.0.252	IGMPv2	46	Membership Report group 224.0.0.252
26	73.054550	192.168.1.9	224.0.0.252	IGMPv2	46	Membership Report group 224.0.0.252

```
[Frame is marked: False]
[Frame is ignored: False]
[Protocols in frame: eth:ethertype:ip:udp:data]
[Coloring Rule Name: UDP]
[Coloring Rule String: udp]
✓ Ethernet II, Src: IntelCor_64:ba:04 (a8:6d:aa:64:ba:04), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
  > Destination: Broadcast (ff:ff:ff:ff:ff:ff)
  > Source: IntelCor_64:ba:04 (a8:6d:aa:64:ba:04)
    Type: IPv4 (0x0800)
  > Internet Protocol Version 4, Src: 192.168.1.9, Dst: 255.255.255.255
  > User Datagram Protocol, Src Port: 58915, Dst Port: 2002
    Source Port: 58915
    Destination Port: 2002

0000  ff  ff  ff  ff  ff  ff  a8  6d  aa  64  ba  04  00  00  45  00  .....d...E.
0010  00  00  ff  ff  b7  00  00  00  00  00  00  00  00  00  00  00  00  .....
0020  ff  ff  e6  23  07  42  00  1c  6e  28  31  30  30  30  30  30  30  .....1|100000
0030  30  31  30  31  30  30  31  30  31  30  31  31  30  31  01010001 001010
```

```

0000  ff ff ff ff ff ff a8 6d  aa 64 ba 04 08 00 45 00  .....m..d...E-
0010  00 30 47 b7 00 00 80 11  00 00 c0 a8 01 09 ff ff  -0G...1.....
0020  ff ff e6 23 07 d2 00 1c  6c 28 31 30 30 30 30 30  -#.....1(100000
0030  30 31 30 31 30 30 30 31  30 30 31 31 30 31 31 31  01010001 001101

```

Wireshark tool used to track packets



F-16 Fighting Falcon

Conclusions

In conclusion, there is more to be discovered with this research. I know there are many vulnerabilities within MIL-STD-1553 and once they are exploited, attackers may grab the control of flying objects. With there being no form of authentication methods in the simulator, encryption and decryption methods will have to be put in place. This will cause a delay in the simulator that will have an unknown effect of the protocol. Mitigation strategies must be properly designed and integrated into the system to protect the protocol and our pilots.

References

Kulkarni, Shubhankar. "Merge Pull Request #2 from ShubhankarKulkarni/Add-License-1 · ShubhankarKulkarni/MIL-STD-1553-Simulator@6ec924f." *GitHub*, 23 Apr. 2021, github.com/ShubhankarKulkarni/MIL-STD-1553-Simulator/commit/6ec924f1b289be4879e1769a03a0b06d8f43a560.

Santo, D. De, et al. "Exploiting the MIL-STD-1553 Avionic Data Bus with an Active Cyber Device." *Computers & Security*, Elsevier Advanced Technology, 27 Oct. 2020. www.sciencedirect.com/science/article/pii/S0167404820303709.

Randazzo, Michael. "Solving Cyber Security on Avionics Databusses." *AIM-Online*, www.aim-online.com/wp-content/uploads/2018/10/aim-ef-cyber-security-feature-180803-u-1.pdf.

"What Is MIL-STD-1553?" *MIL*, www.milstd1553.com/.