



***“A Better Space Mission Systems  
threat assessment by leveraging  
the National Cyber Range”***

***Chuck Allen (CISSP) & Jonathon Doubleday  
CORD***

***Presented to GSAW, Feb-March 2018***

## ***Abstract***

Aerospace cyber SME's successfully led efforts to bring the first major comprehensive cyber assessment of the Space Mission Architecture into the National Cyber Range.

The National Cyber Range (NCR) is a DoD owned national asset with the aim of providing realistic cyber simulation, assessment and modeling.

Efforts will help advance cyber research, optimize defensive cyber operations and enhance space mission resilience.

SSDP



# Briefing Outline

- The National Cyber Range
- The Space Virtual mission Environment
- Cyber exploits
- Vulnerability mitigations
- Summary / conclusions

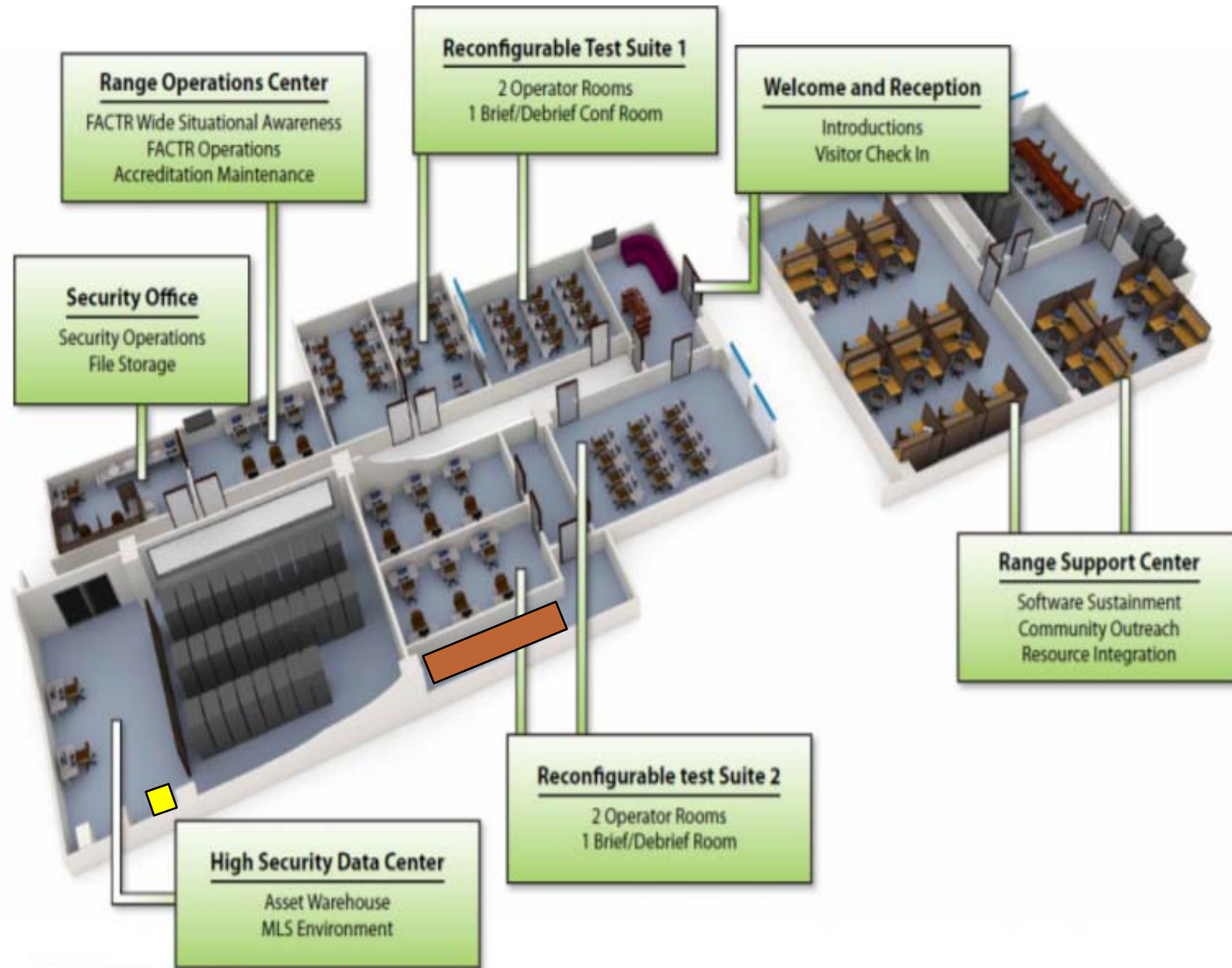


*National Cyber Range, Florida*

***It's a race to find the space cyber vulnerabilities before the bad guys do***



# NCR Layout



## ***Our approach: We brought our unique equipment, NCR provides the Infrastructure and Cyber Adversaries....Fights on!***

- SSDP Provided the Front End Processors and objectives
- NCR provided the:
  - Cyber Security Exploit Team (CSET) to assess the Front End Processors
  - Network shown in the Tested Environment

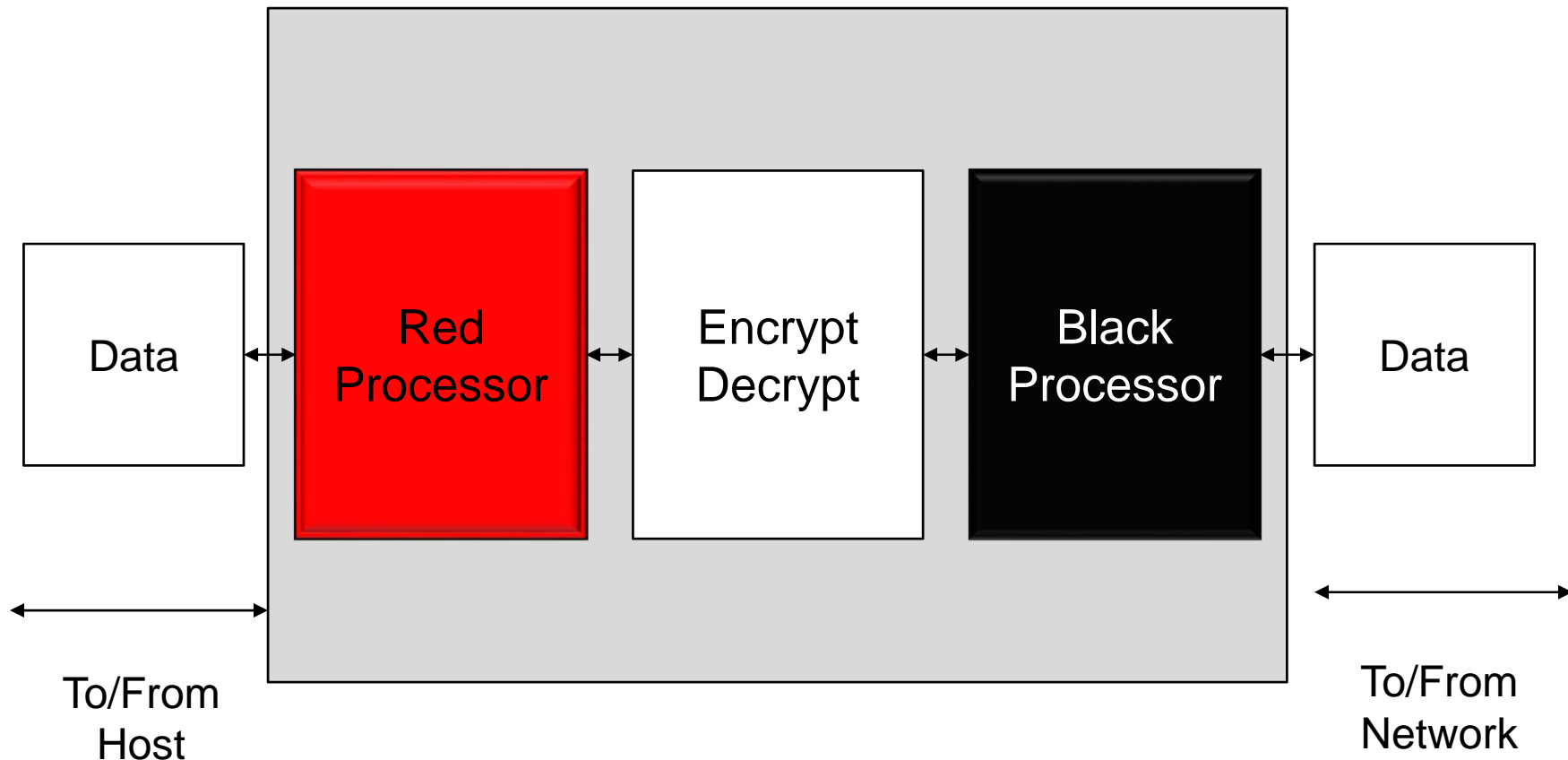


Source: [http://www.acq.osd.mil/dte-trmc/docs/20150224\\_NCR%20Overview\\_DistA.pdf](http://www.acq.osd.mil/dte-trmc/docs/20150224_NCR%20Overview_DistA.pdf)

***NCR Server Room***

Source: [https://res.cloudinary.com/dodge7ws8/image/upload/t\\_carousel-large/v1487348076/reporter/live/tree-imports/VISUAL04548/Crash\\_test\\_dummy\\_visual.jpg](https://res.cloudinary.com/dodge7ws8/image/upload/t_carousel-large/v1487348076/reporter/live/tree-imports/VISUAL04548/Crash_test_dummy_visual.jpg)

# Top Level Architecture



*Purpose built computers that manage a communication to and from a computer system*

## ***Cyber Threat Vectors employed:***

- Reconnaissance: Network scans
- Surveillance: Network Presence
- Access, lateral movement and actual exploits:

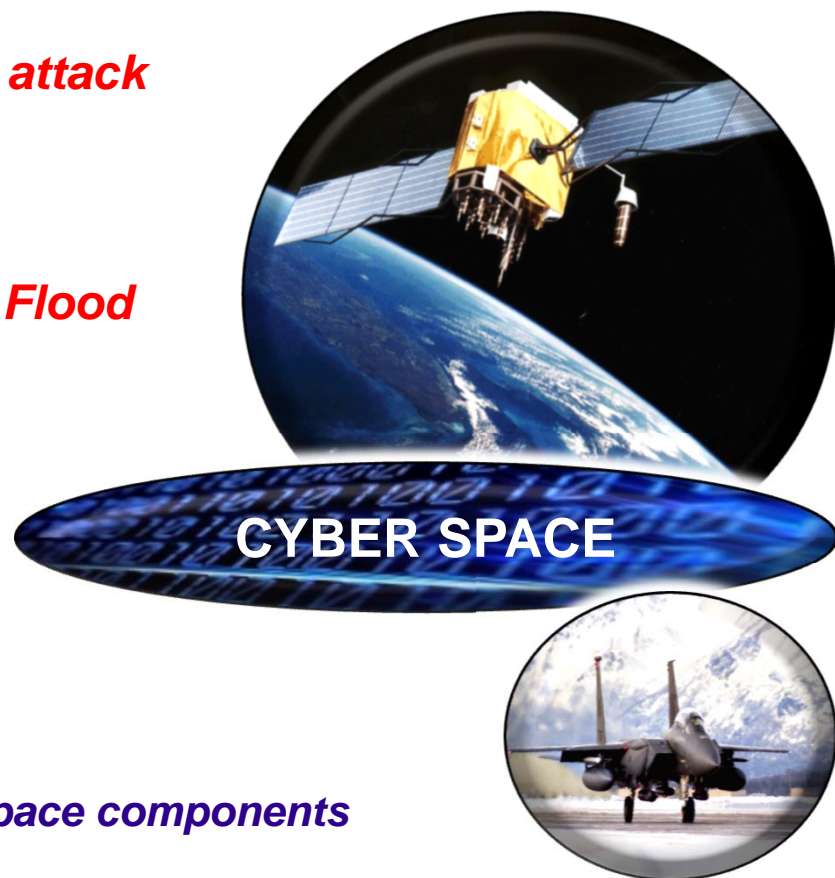
***1. Out-of-Band Management network attack***

***2. Man in the Middle***

***3. Secure Shell (SSH) Authentication Flood***

***4. Denial of Service (massive Logs)***

***5. Physical access (Insider Threat)***



***Bottom line: using real cyber exploits on real Space components***



## Surveillance: Network scans

*Note: iptables enabled which is the “Shields Up configuration”*

- Scanning the network to find potential open ports with iptables enabled and a restricted IP address
- Red FEP Scan results:

```
root@RTkali:14:45> nmap -e eth1 -sS -T5 -n -Pn 10.50.2.10 -oX /root/scans/shieldsup-scan.xml -p-
Starting Nmap 7.40 ( https://nmap.org ) at 2017-05-25 14:45 EDT
Nmap scan report for 10.50.2.10
Host is up (0.00024s latency).
All 65535 scanned ports on 10.50.2.10 are filtered
MAC Address: 34:17:EB:EB:A3:43 (Dell)
Nmap done: 1 IP address (1 host up) scanned in 658.46 seconds
```

- Black FEP IP restricted scan results:

```
root@RTkali:14:45> nmap -e eth1 -sS -T5 -n -Pn 192.168.2.10 -oX /root/scans/shieldsup-scan.xml -p-
Starting Nmap 7.40 ( https://nmap.org ) at 2017-05-25 14:45 EDT
Nmap scan report for 192.168.2.10
Host is up (0.00024s latency).
All 65535 scanned ports on 192.168.2.10 are filtered
Nmap done: 1 IP address (1 host up) scanned in 658.46 seconds
```



Use Iptables to restrict the number of ports exposed to the bare minimum.  
With a non restricted IP scans only showed SSH (port 22) and NTP (port 123)

***Scans did not turn up any information in the hardened “Shields Up” state, however system used two ports (i.e. SSH and Timing)***



# Network Presence

## *Out of Band Management*

- Out-of-Band Management (OOB) widely used for remote access into networks
- Out-of-Band Management could be vulnerable if not configured properly





# Man in the Middle

## ARP (Address Resolution Protocol) spoofing

- Use ARP spoofing to create disruptions
- However, use of properly configured SSH will protect integrity and confidentiality

No.	Time	Source	Destination	Protocol	Length	Info
4535	185.152202255	10.58.2.10	19.50.2.100	TCP	118	[TCP Retransmission] 22 → 58824 [PSH, ACK] Seq=4
4537	185.167499519	10.58.2.100	19.50.2.10	SSH	214	Client: Encrypted packet (len=148)
4538	185.167928964	10.58.2.100	19.50.2.10	TCP	214	[TCP Retransmission] 58824 → 22 [PSH, ACK] Seq=3
4539	185.168168293	10.58.2.10	19.50.2.100	SSH	1334	Server: Encrypted packet (len=1268)
4543	185.179066858	10.58.2.10	19.50.2.100	TCP	1334	[TCP Retransmission] 22 → 58824 [PSH, ACK] Seq=4
4541	185.188264744	10.58.2.100	19.50.2.10	SSH	182	Client: Encrypted packet (len=116)
4542	185.191895881	10.58.2.100	19.50.2.10	TCP	182	[TCP Retransmission] 58824 → 22 [PSH, ACK] Seq=3
4543	185.192103373	10.58.2.10	19.50.2.100	SSH	262	Server: Encrypted packet (len=196)
4544	185.199981355	10.58.2.10	19.50.2.100	TCP	262	[TCP Retransmission] 22 → 58824 [PSH, ACK] Seq=4
4545	185.200219815	10.58.2.100	19.50.2.10	SSH	438	Client: Encrypted packet (len=354)
4546	185.206198175	10.58.2.100	19.50.2.10	TCP	438	[TCP Retransmission] 58824 → 22 [PSH, ACK] Seq=3
4547	185.206444182	10.58.2.10	19.50.2.100	SSH	214	Server: Encrypted packet (len=148)
4548	185.216119861	10.58.2.10	19.50.2.100	TCP	214	[TCP Retransmission] 22 → 58824 [PSH, ACK] Seq=4
4549	185.255767488	10.58.2.100	19.50.2.10	TCP	66	58824 → 22 [ACK] Seq=329261 Ack=483729 Win=3862
4550	185.269915873	10.58.2.100	19.50.2.10	TCP	66	[TCP Dup ACK 4549#] 58824 → 22 [ACK] Seq=329261
4551	185.284158262	10.58.2.10	19.50.2.100	SSH	574	Server: Encrypted packet (len=538)
4552	185.276037833	10.58.2.10	19.50.2.100	TCP	574	[TCP Retransmission] 22 → 58824 [PSH, ACK] Seq=4
4553	185.276336773	10.58.2.100	19.50.2.10	TCP	66	58824 → 22 [ACK] Seq=329261 Ack=483729 Win=3862
4554	185.283948525	10.58.2.100	19.50.2.10	TCP	66	[TCP Dup ACK 4553#] 58824 → 22 [ACK] Seq=329261
4555	185.418818498	10.58.2.100	19.50.2.10	SSH	214	Client: Encrypted packet (len=148)

Frame 4555: 214 bytes on wire (1712 bits), 214 bytes captured (1712 bits) on interface 8

- Ethernet II, Src: VMware\_a9:e8:ce (00:50:56:a9:e8:ce), Dst: VMware\_a9:e7:d6 (08:5b:56:a9:e7:d6)
- Internet Protocol Version 4, Src: 10.58.2.100, Dst: 19.50.2.10
- Transmission Control Protocol, Src Port: 58824, Dst Port: 22, Seq: 329261, Ack: 483729, Len: 148
- SSH Protocol

0000 30 50 56 a9 e7 d6 00 50 56 a9 e8 ce 08 03 45 00 Pv...P.V....E  
0010 30 c8 77 dc 48 09 40 08 a9 e2 ba 32 62 64 0a 32 v.B.@....2.d.2  
0020 32 0a e5 c8 08 16 13 16 9a d6 e2 91 ee 84 80 18  
0030 3c f8 4f c5 06 03 01 01 08 0a 85 26 87 a1 05 8a O.....&...  
0040 a9 03 f9 ca 1d b3 98 d8 ce b5 c3 94 02 4c 27 95 c...X....BL'  
0050 88 dd d7 c6 77 ff 48 11 t:18.44.07.6f.aa.32.51 n.w.H.D.o.2V

# Network Mitigations

- Mitigating Man in the Middle (ARP spoof)
- SSH Authentication flood Mitigation
  - Separate the remote login from the local login account
- Denial of Service Log Mitigation
  - Prevent /var/log and /var/log/audit locations filling up by overwriting older log files
  - Creating a warning when log locations are filled to a set level



# Conclusion / Summary of leveraging the NCR

## National Cyber Range FEP Threat/Cyber Assessment



NCR	Key Highlights
<b>Innovation</b>	<ul style="list-style-type: none"><li>• Serves as pathfinder for future cyber / threat assessments</li></ul>
	<ul style="list-style-type: none"><li>• First major Space Mission architecture leveraging the NCR</li></ul>
<b>Velocity</b>	<ul style="list-style-type: none"><li>• Compresses normal assessment times from 9 months to 3 months</li></ul>
<b>Flexibility</b>	<ul style="list-style-type: none"><li>• Able to quickly create multiple assessments at different classification environments</li></ul>
	<ul style="list-style-type: none"><li>• Immersive, dynamic, operational cyber environment</li></ul>
<b>Cost savings</b>	<ul style="list-style-type: none"><li>• SSDP saved \$500K in cost avoidance by using the NCR vice creating an internal test development network</li></ul>
<b>Better results</b>	<ul style="list-style-type: none"><li>• Capability to identify &amp; isolate vulnerabilities but also demonstrate efficacy of fix actions</li></ul>





## ***For more information***

- For additional classified information of the cyber assessment please email:
- Charles T. Allen, CISSP
  - Charles.T.Allen@Aero.org
- Jonathon Doubleday
  - Jonathon.S.Doubleday@aero.org



## Questions?

