



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

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

Presented to GSAW, Feb 2019



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.



Briefing Outline

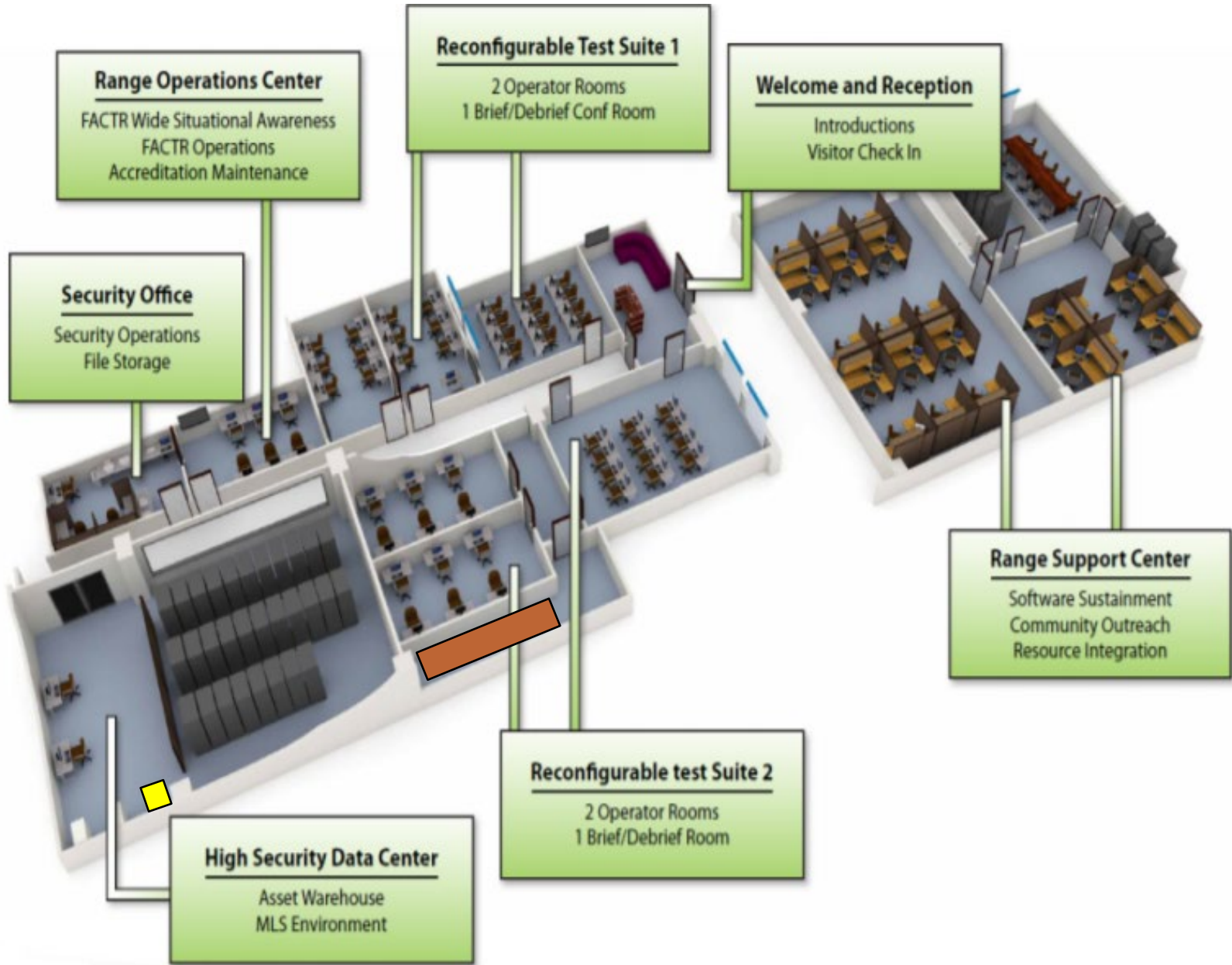


- The National Cyber Range
- The Space Virtual mission Environment
- Cyber exploits
- Vulnerability mitigations
- Summary / conclusions



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



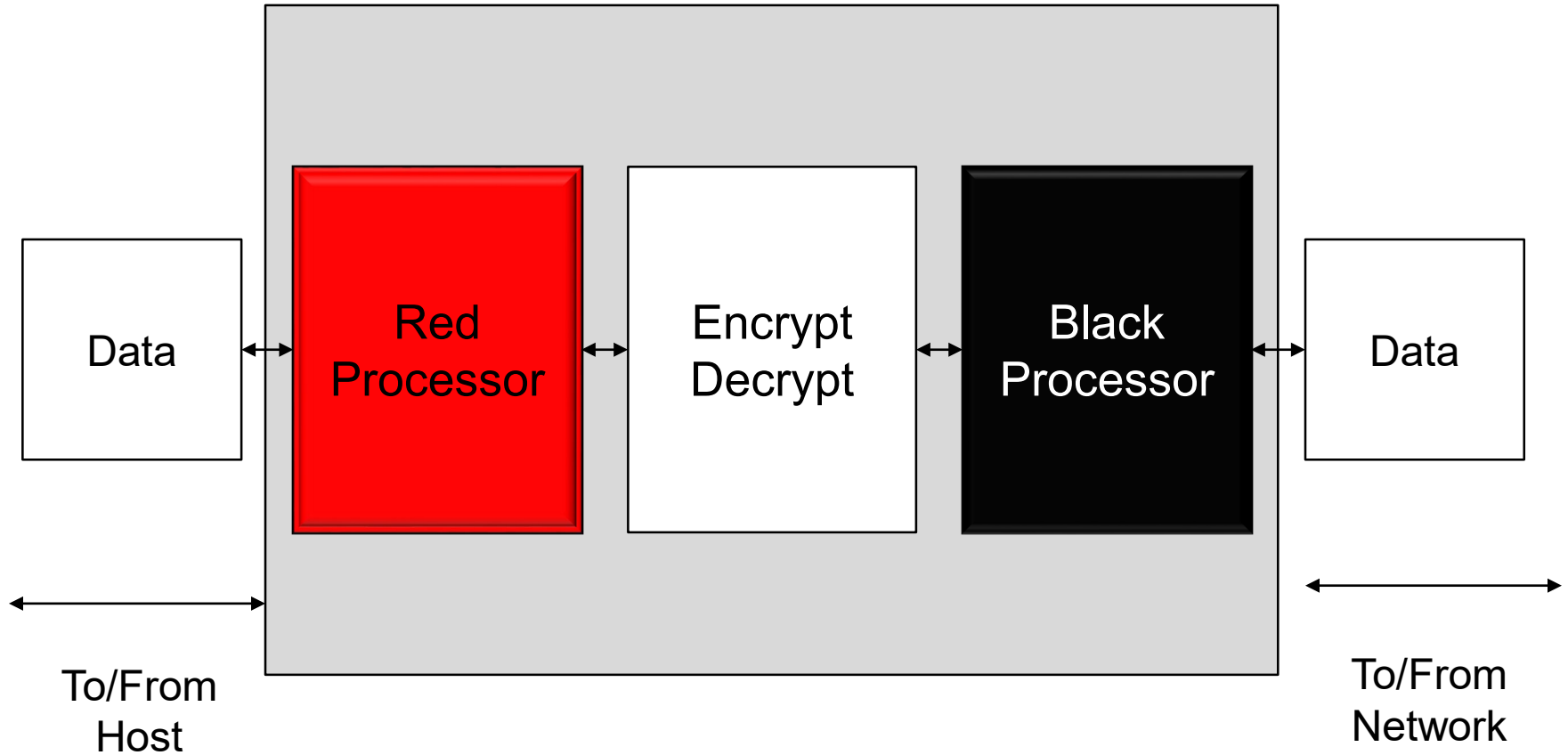
Source: http://www.acq.osd.mil/dte-trmc/docs/20150224_NCR%20Overview_DistA.pdf

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

Top Level Architecture

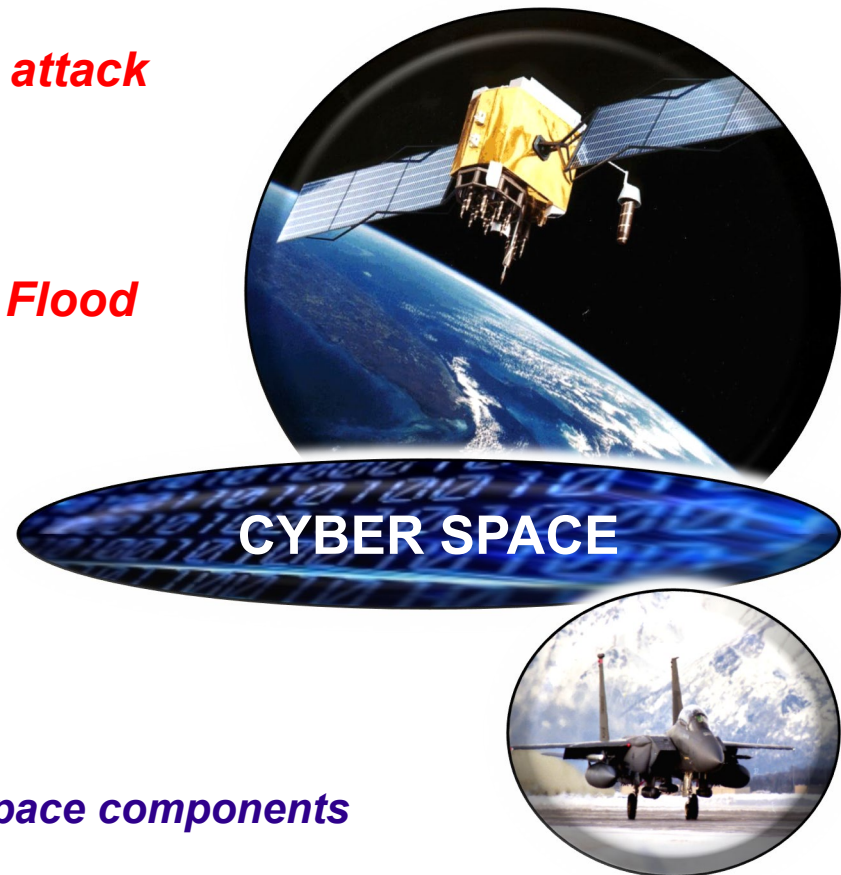


Purpose built computers that manage a communication to and from a computer system



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

The screenshot shows the Wireshark interface with a list of network packets. The interface includes a menu bar (File, Edit, View, Go, Capture, Analyze, Statistics, Telephony, Wireless, Tools, Help), a toolbar, and a display filter field. The packet list table is as follows:

No.	Time	Source	Destination	Protocol	Length	Info
4535	185.152202255	10.58.2.10	10.50.2.100	TCP	118	[TCP Retransmission] 22 → 58824 [PSH, ACK] Seq=4
4537	185.167499519	10.58.2.100	10.50.2.10	SSH	214	Client: Encrypted packet (len=148)
4538	185.167928964	10.58.2.100	10.50.2.10	TCP	214	[TCP Retransmission] 58824 → 22 [PSH, ACK] Seq=3
4539	185.168168293	10.58.2.10	10.50.2.100	SSH	1334	Server: Encrypted packet (len=1268)
4540	185.178006358	10.58.2.10	10.50.2.100	TCP	1334	[TCP Retransmission] 22 → 58824 [PSH, ACK] Seq=4
4541	185.188264744	10.58.2.100	10.50.2.10	SSH	182	Client: Encrypted packet (len=116)
4542	185.191895891	10.58.2.100	10.50.2.10	TCP	182	[TCP Retransmission] 58824 → 22 [PSH, ACK] Seq=3
4543	185.192183373	10.58.2.10	10.50.2.100	SSH	262	Server: Encrypted packet (len=196)
4544	185.199981355	10.58.2.10	10.50.2.100	TCP	262	[TCP Retransmission] 22 → 58824 [PSH, ACK] Seq=4
4545	185.200219815	10.58.2.100	10.50.2.10	SSH	438	Client: Encrypted packet (len=354)
4546	185.206198175	10.58.2.100	10.50.2.10	TCP	438	[TCP Retransmission] 58824 → 22 [PSH, ACK] Seq=3
4547	185.206444182	10.58.2.10	10.50.2.100	SSH	214	Server: Encrypted packet (len=148)
4548	185.216119661	10.58.2.10	10.50.2.100	TCP	214	[TCP Retransmission] 22 → 58824 [PSH, ACK] Seq=4
4549	185.255767489	10.58.2.100	10.50.2.10	TCP	66	58824 → 22 [ACK] Seq=329261 Ack=483729 Win=3862
4550	185.263915873	10.58.2.100	10.50.2.10	TCP	66	[TCP Dup ACK 4549#] 58824 → 22 [ACK] Seq=329261
4551	185.264158262	10.58.2.10	10.50.2.100	SSH	574	Server: Encrypted packet (len=538)
4552	185.270037833	10.58.2.10	10.50.2.100	TCP	574	[TCP Retransmission] 22 → 58824 [PSH, ACK] Seq=4
4553	185.276336779	10.58.2.100	10.50.2.10	TCP	66	58824 → 22 [ACK] Seq=329261 Ack=483729 Win=3862
4554	185.283948529	10.58.2.100	10.50.2.10	TCP	66	[TCP Dup ACK 4553#] 58824 → 22 [ACK] Seq=329261
4555	185.416318498	10.58.2.100	10.50.2.10	SSH	214	Client: Encrypted packet (len=148)

Below the packet list, the details pane shows the structure of frame 4555:

- 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 (00:50:56:a9:e7:d6)
- Internet Protocol Version 4, Src: 10.58.2.100, Dst: 10.50.2.10
- Transmission Control Protocol, Src Port: 58824, Dst Port: 22, Seq: 329261, Ack: 483729, Len: 148
- SSH Protocol

The packet bytes pane shows the raw data in hexadecimal and ASCII:

```
0000 00 50 56 a9 e7 d6 00 50 56 a9 e3 ce 08 00 45 00  P.V.V...E
0010 00 c8 77 cc 48 00 40 06 a9 82 9a 32 02 64 0a 32  w.@...2.d.2
0020 02 0a e5 c8 08 16 13 16 9a d8 e2 9f ee 84 80 18  .....
0030 0e f6 4f c5 08 00 01 01 08 0a 05 28 07 a1 05 8a  .O.....&....
0040 a9 63 f9 ca 1d b3 58 d8 ce b5 c3 94 62 4c 27 05  c...X...BL^
0050 88 dd d7 c6 77 ff 48 11 e1 18 44 07 6f ea 32 51  t...w.H...D.o.2
```



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



For more information

- For additional classified information of the cyber assessment please email:
- Charles T. Allen, CISSP
 - GWAN / NMIS / JWICS:
- Jonathon Doubleday
 - CWAN / ASEnet:



Questions?

