"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

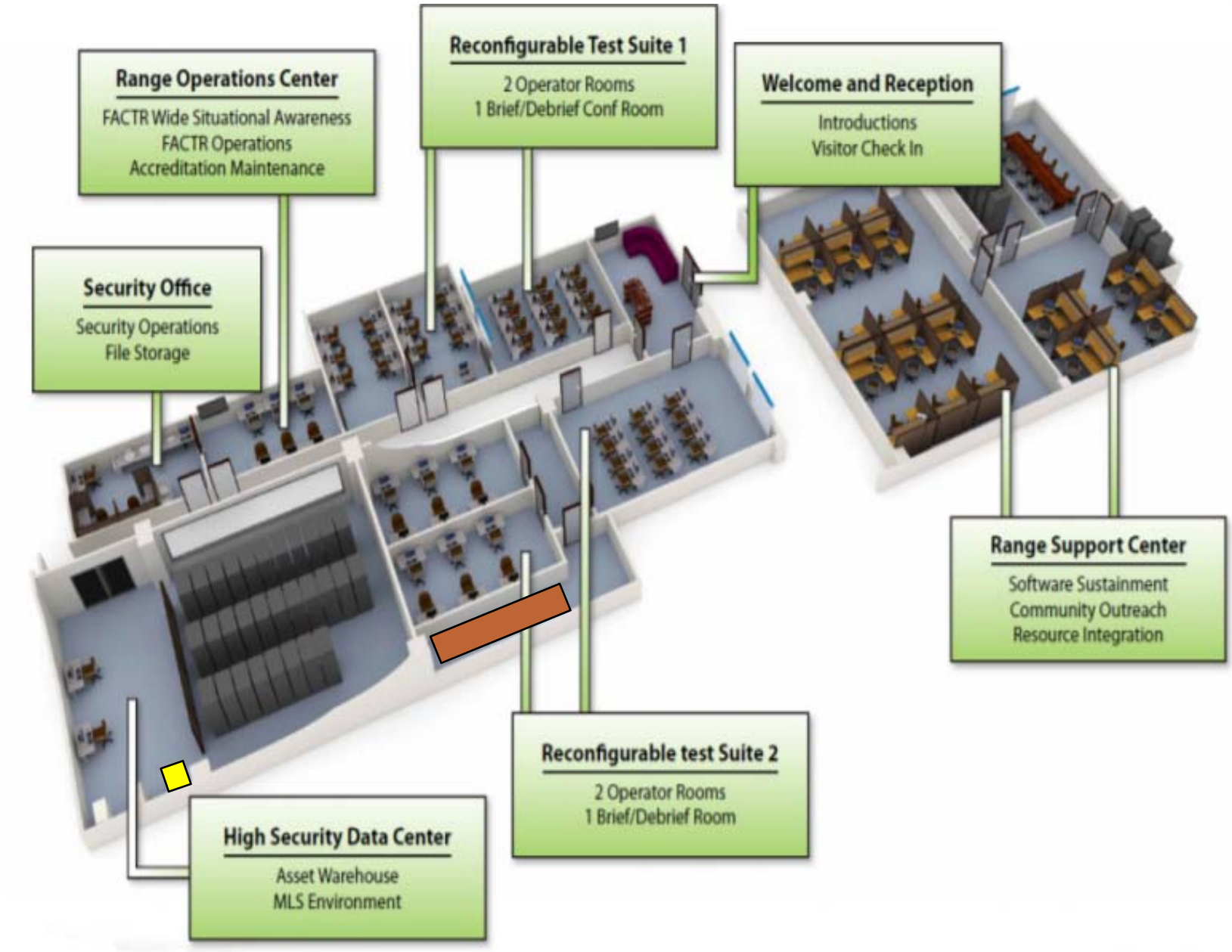
Briefing Outline

- 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


Range Operations Center
FACTR Wide Situational Awareness
FACTR Operations
Accreditation Maintenance
Reconfigurable Test Suite 1
2 Operator Rooms
1 Brief/Debrief Conf Room
Welcome and Reception
Introductions
Visitor Check In
Security Office
Security Operations
File Storage
Range Support Center
Software Sustainment
Community Outreach
Resource Integration
Reconfigurable test Suite 2
2 Operator Rooms
1 Brief/Debrief Room
High Security Data Center
Asset Warehouse
MLS Environment

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

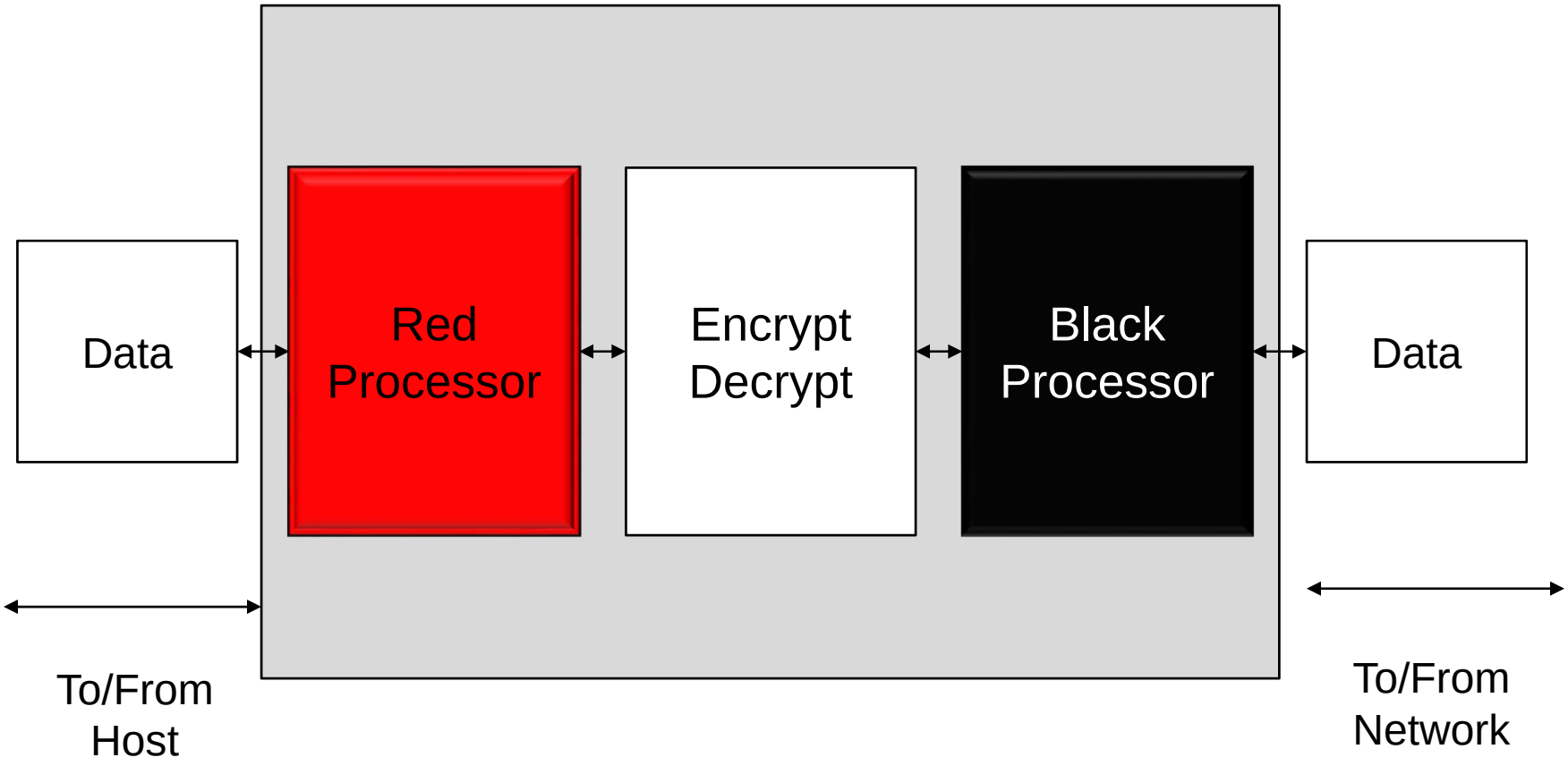
  - Network shown in the Tested Environment

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

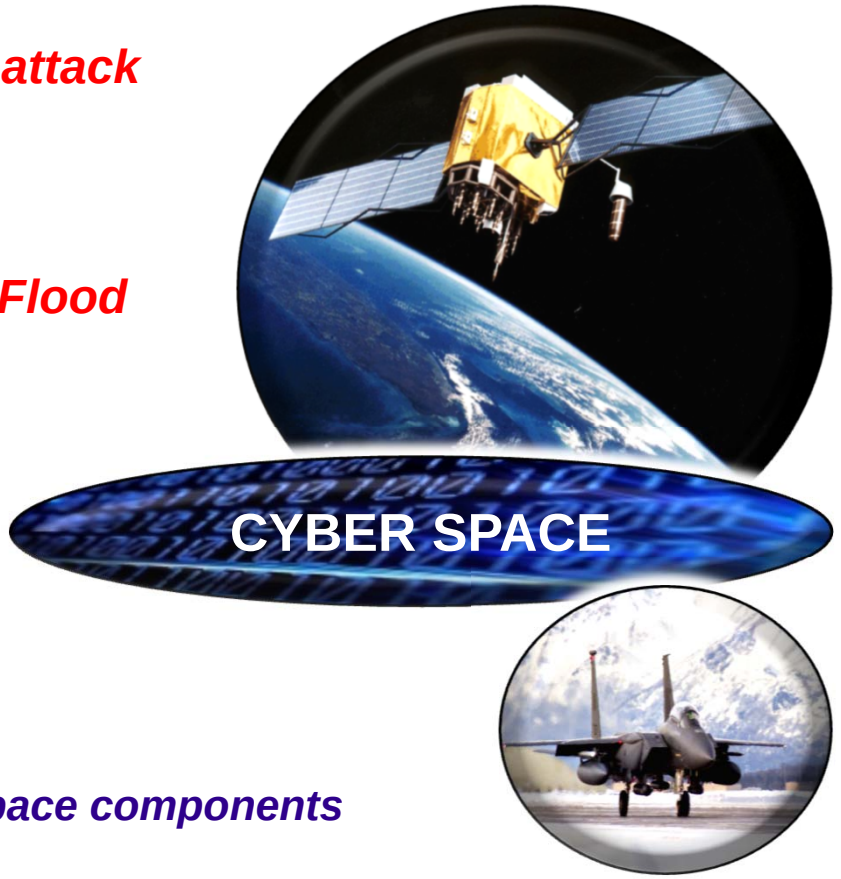


Purpose built computers that manage a communication to and from a computer system

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

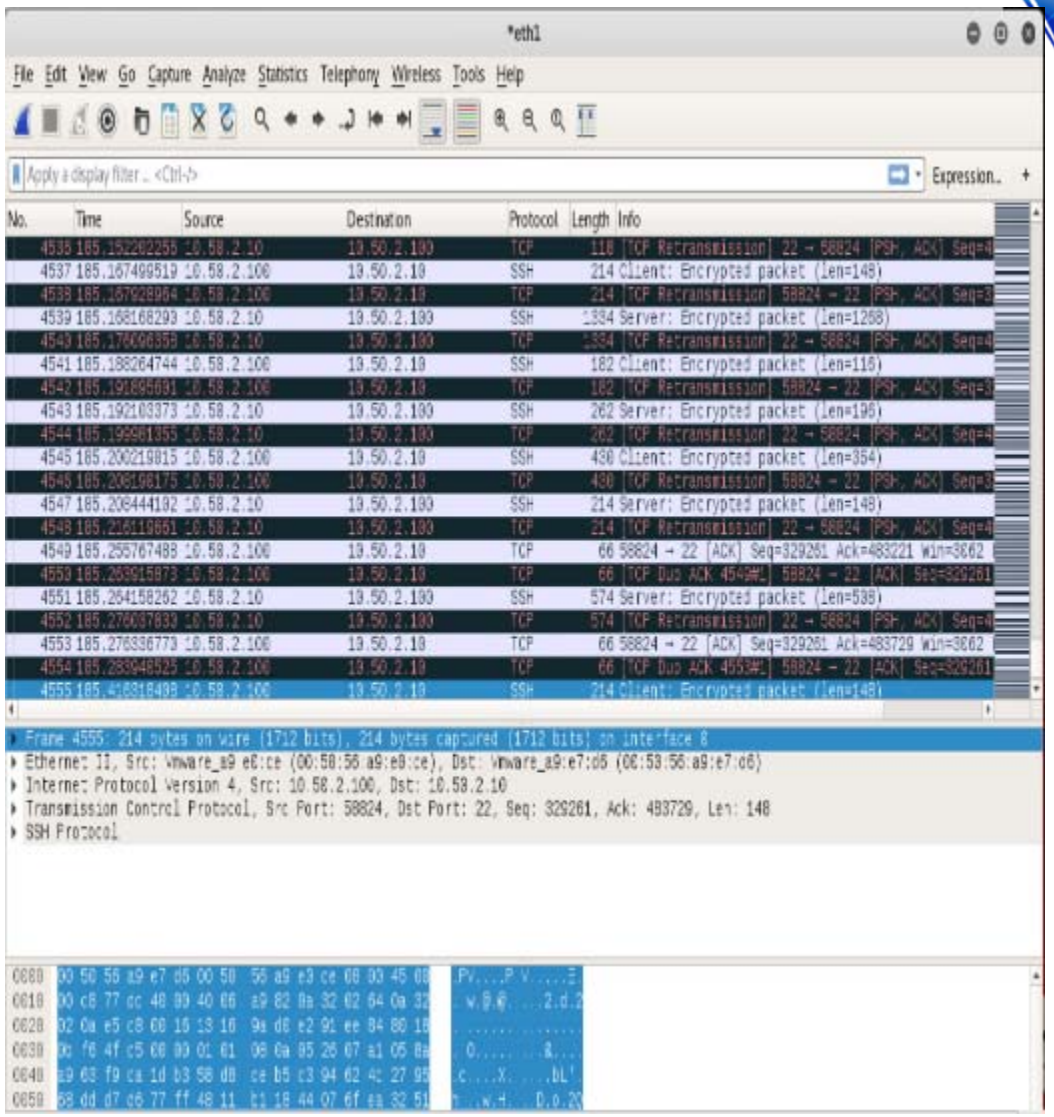
Out of Band Management

- 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



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
Innovation	• Serves as pathfinder for future cyber / threat assessments
	• First major Space Mission architecture leveraging the NCR
Velocity	• Compresses normal assessment times from 9 months to 3 months
Flexibility	• Able to quickly create multiple assessments at different classification environments
	• Immersive, dynamic, operational cyber environment
Cost savings	• SSDP saved $500K in cost avoidance by using the NCR vice creating an internal test development network
Better results	• 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
  - Charles.T.Allen@Aero.org

- Jonathon Doubleday
  - Jonathon.S.Doubleday@aero.org

Questions?