CYBERSECURITY OT&E

Briefing for the ITEA 2nd Cyber Security Workshop:
"Test and Evaluation to Meet the Advanced Persistent Threat"

Dr Mitch Crosswait
Deputy Director, OT&E

PlayStation™

WE ARE ANONYMOUS

DOT&E Cybersecurity Roles

- Cybersecurity OT&E of systems during acquisition
  - DOT&E Memo "*Procedures for the Operational Test and Evaluation of Cybersecurity in Acquisition Programs*" (1 Aug 2014)
    - Specifies a two-phase OT&E: *Cooperative Vulnerability and Penetration Assessment* followed by an *Adversarial Assessment*
    - Goal: Identify all significant vulnerabilities and operational impact
- Cybersecurity operational assessments
  - Congressional mandate (FY03 DAA, October 2002)
  - Conduct cybersecurity assessment at each CCMD and Service at least once annually during a major exercise
    - Over 200 assessments conducted since 2003
    - Aggregate results analyzed annually and reported
- *Cybersecurity ranges and training*
  - Joint Information Operations Range
  - CMF/CPT Training support

DOT&E Cybersecurity Findings

- Both acquisition and exercise events point to the same findings:
  - Passwords and other credentials are readily available to intruders
  - Software is often not up-to-date
  - Software is frequently not configured properly for security
  - Networks and applications have services and capabilities enabled that are easily exploited
- Most cybersecurity vulnerabilities discovered during OT could have / should have been discovered during EMD/DT
  - 90% of all cybersecurity findings FY12-FY14 did not require operational testing to discover

What Makes a Good Test?

A good test results in the resolution of shortfalls and identify the reasons some shortfalls persist. It needs:

- *A Representative System*: the system must be equivalent to the system that will be fielded, and fielded in a way that is consistent with the operational CONOPs
- *The Representative Threat*: the system must be assessed for the ability to "fight through" while exposed to the cyber threats that have been identified for the system and/or network
- *Representative users*: the system must be tested while being operated by typical users with typical levels of training and inherent expertise
- *Deconfliction*: the cybersecurity tests should be deconflicted from other test objectives so that the findings are not constrained or limited.
- *Time*: the test needs to be long enough to meet data requirements

Problems With Representative Systems

- Platform shortages:
  - The typical platform is not available due to operations or a mismatch in delivery schedules
- Configuration issues:
  - The software is not locked (still open to revisions)
  - The software is still a developmental load
  - The software is not the version that will be fielded
- Environmental/Architectural issues:
  - The software is not installed on an operationally representative network (or there is not representative network available)

Threat Challenges

- Asset shortages – not enough Red/Blue Teams available
  - Expansion of operational cyber teams is hurting the availability of skilled cyber teams for acquisition testing
- Intelligence and enumeration:
  - The test teams must conduct extensive discovery of the network and systems to accommodate testing
  - System Threat Assessment Reports (STARs) do not cover
- Execution issues:
  - Permissions: ROE and ground rules are required for every event and cannot be too restrictive.
    - Makes “fighting through” difficult to assess
  - Safety: software decertification risks; open networks

Challenges With Other Resources

- Representative users not available:
  - Either an availability or a training issue
  - Inclusion of Tier 2 and Tier 1 cyber defenders can be both an advantage and an artificiality
  - Most users are not trained to distinguish cyber effects from simple malfunctions or maintenance issues
- Cyber tests cannot be deconflicted from other events:
  - Cannot combine flight hours / availability tests with cyber tests that may make the aircraft software unsafe
  - Need to set aside specific opportunities to demonstrate cyber mission effects
- Timing is everything:
  - The best test results in fixing things – cannot accomplish if the testing phases are too close together
  - Duration of the test is too short to depict the full threat

Potential Solutions

- Cyber ranges
  - “Safe sandbox” ranges allow depiction of more aggressive/realistic threats and more realistic cyber defenses
  - Ability to demonstrate cyber mission effects without adversely affecting an operational platform
- Persistent Cyber Threats
  - Extends exposure of Red/Blue activities
  - Allows for re-use of key architecture assessments
  - Requires extensive prior coordination, but less event coordination
- Dedicated test systems / events
  - While more resource-intensive, dedicated cybersecurity test articles and test events allow rapid completion of tests without interference with other objectives


THE WEAPONS AT THEIR FINGERTIPS
10,000 BC
10 BC
1500 AD
1700 AD
1910 AD
SURFACE TO AIR
2010 AD
TODAY
DRONE STRIKE
CYBER-ATTACK
KAL