(U//FOUO) Net Defense from Encrypted Communications

February 2013
Increment 3 Requirement

SYSREQ10322.2
(S//REL) TURMOIL shall reinject decrypted IP traffic into BLUESNORT for malicious network activity detection.
Three-Feather Solution

1. **GALLANTWAVE application**
   - Same module supports NetDef and SIGINT
   - Supports dynamic update of targeting via UTT
   - Supports static target updates

2. **GALLANTWAVE Reinjection application**
   - Same module supports NetDef and SIGINT
   - Supports re-injection of decrypt into TURMOIL for detection by BLUESNORT

3. **BLUESNORT in Stage 1 Prime application**
   - Emits events off decrypted, re-packetized, reinjected data
HIGH Level Data Flow
Net Defense and SIGINT sites

UTT ------~-. -.
TURMOIL/ Mission Application
~

PITBOSS -------y-- ----->

GALLANTWAVE
CA Server
GALLANTWAVE REINJECTION
BLUESNORT

TIPS (Bluesnort Events)

LONGHAUL
XKEYSCORE
Status

- Running on MHS DEV ESO T5 and T22
- Transform, Reinjection, Signature Hits confirmed
- Signatures need further development to produce true hits vs. false positives
- NTOC POC reviewing XKS hits to generate new signatures.
Issues/Risks

1. CA Servers at Net Defense Sites
   a) ITx Connectivity to LONGHAUL
   b) NTOC requires stand-up of separate dev and live ITx fabric
      i. H/W funding may be needed
      ii. Need paperwork for update to firewall – submission expected by 25 Feb
   c) Expected completion was 29 Feb; now delayed to TBD
   d) SSH connectivity
      i. Short term: via BLUEBOX CA Servers at Pentagon - done
      ii. Longer term: via deployment of servers within the NTOC enclave that connect to CA Servers in the field

2. GALLANTWAVE Targeting Challenges
   a) MAILORDER/Ni-Fi not yet available
   b) Mitigation: Manually load static targeting files
CA Capabilities Planned for NCC-3 Test Events

<table>
<thead>
<tr>
<th>Capability</th>
<th>DT/OA 2 (June 2012)</th>
<th>DT/OA 3 (June 2013)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Defensive Sensor</td>
<td></td>
<td></td>
</tr>
<tr>
<td>SIGINT Sensor</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Defensive Sensor</td>
<td></td>
<td></td>
</tr>
<tr>
<td>SIGINT Sensor</td>
<td></td>
<td></td>
</tr>
<tr>
<td>CA Reinjection</td>
<td>No</td>
<td>DGO</td>
</tr>
<tr>
<td></td>
<td></td>
<td>TTENT</td>
</tr>
<tr>
<td></td>
<td></td>
<td>DGO</td>
</tr>
</tbody>
</table>
# Near-term Schedule

<table>
<thead>
<tr>
<th>Capability</th>
<th>Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>GW-R Gate 2</td>
<td>Done (15 Feb)</td>
</tr>
<tr>
<td>GW-R Gate 3</td>
<td>Done (29 Feb)</td>
</tr>
<tr>
<td>GW-R Gate 5</td>
<td>31 Mar</td>
</tr>
<tr>
<td>GW-R Deploy to U sites</td>
<td>May</td>
</tr>
<tr>
<td>ITx Dev Fabric at NetDef sites</td>
<td>29 Feb +</td>
</tr>
<tr>
<td>CA Server ssh connectivity</td>
<td>Done via Bluebox</td>
</tr>
<tr>
<td>Initial Live Dev Test TURTLEZOO</td>
<td>~May</td>
</tr>
<tr>
<td>GW-R Core 4.0</td>
<td>May</td>
</tr>
<tr>
<td>GW Core 4.0</td>
<td>May</td>
</tr>
<tr>
<td>ITx Live Fabric</td>
<td>TBD</td>
</tr>
</tbody>
</table>
Players
BACKUP SLIDES
CCA Capabilities Planned for NCC-3 Test Events

<table>
<thead>
<tr>
<th>Capability</th>
<th>DT/OA 2 (June 2012)</th>
<th>DT/OA 3 (June 2013)</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Defensive Sensor</td>
<td>SIGINT Sensor</td>
</tr>
<tr>
<td>-----------------------------------------</td>
<td>-----------------</td>
<td>-------------------------------</td>
</tr>
<tr>
<td>NETFLOW</td>
<td>Full Netflow</td>
<td>Pretty Good Netflow</td>
</tr>
<tr>
<td>BLUESNORT (updates)</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>FULL SNORT</td>
<td>Yes</td>
<td>No (Core 4)</td>
</tr>
<tr>
<td>POPQUIZ</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>Performance Testing</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>Wireless reinjection</td>
<td>N/A</td>
<td>Yes</td>
</tr>
<tr>
<td>CA Reinjection</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>Cyber Tasking</td>
<td>Yes</td>
<td>Partial</td>
</tr>
<tr>
<td>Updated Cloudshield Interface</td>
<td>Partial</td>
<td>N/A</td>
</tr>
<tr>
<td>Metrics and Monitoring</td>
<td>Yes</td>
<td>No</td>
</tr>
</tbody>
</table>

Orange items are being revisited. Requirements without explicit TML Core 4 dependency need mission documentation to justify not being covered in DT/OA 2.
Dynamic Defense Logical Diagram

INTERNET

Active Response
Block, Reroute, Alter

CloudShield

TUMULT Stage 0

Network Interface
Normalized Packets

Detect

BUSINESS LOGIC

TURMOIL Stage 1

Alert

Command

TUMULT (T113)
TURMOIL (T112)
TUTELAGE (T111)
NTOC (VSPO)

Legend:
1) CoreSSC gets UTT updates, triggers TA targets
2) GW-TargetManager responds to load targets request from CoreSSC, pulls the GW IP addresses from the Targeting database; issues control-flow messages for each IP:Port combination and sends periodic updates for those.
3) FCP responds to control-flow messages by promoting all packets to/from the targeted IP:port combinations, and PacketRouter ensures these packets are sent to GW-FIP for sessionization. GW-FIP outputs 'raw' SOTF session-fragments to the TE-GW service on the same host.
4) GW-SessionFilter identifies sessions containing target technology-of-interest by applying an appropriate appld tag to each session-fragment.
5) GW-FragmentFilter removes session-fragments not containing an appropriate appld for the target technology-of-interest. Additionally, as a work-around for an issue in FIP 3.1.10, erroneous session-fragments missing a specific metadata field are removed. GW-MI applies SRI obtained from DFID Allocator.
6) GW-MI applies SRI obtained from the DFID allocator.
7) GW-LoadManager delivers buffered data unto a
Delivery to both XKEYSCORE and Stage 1 Prime Reinjection
TURMOIL
Stage 1 Prime Reinjection

Decrypted flow
Reinjection

BLUESNORT

DNS Inspector

HiddenSalamander
e tc ...
Proposed Tasking Flow for TUTELAGE Cryptanalytic Capability

UTT Network Technology

NiFi Corporate Instance

NiFi NTOC Instance

NTOC FIREWALL

CA Server

GALLANTWAVE

TURMOIL

TURMOIL

TUIC

SSDM

NiFi local

LONGHAUL

Key exchange - ITX

IP tasking file / response - SSL

IP tasking file / response - SSL

IP tasking file / response - SSL