Virtual Desktop Infrastructure (VDI)

Contributors:
Suren Karavetttil, Bhumip Khasnabish, Ning So, Russell Wang, Suan Ma, Meng Yu, Zhenping You

Please send comments & suggestions to Suren Karavetttil (surenck@gmail.com)
March 04th, 2010
IETF IPR and Copyright Statements

• This document (future Internet-Draft) is being prepared for IETF in full conformance with the provisions of BCP 78 and BCP 79

• Copyright Notice
  – Copyright (c) 2010 IETF Trust and the persons identified as the document authors. All rights reserved.

• This document is subject to BCP 78 and the IETF Trust's Legal Provisions Relating to IETF Documents in effect on the date of publication of this document (http://trustee.ietf.org/license-info)

•
Outline

• Purpose
• Protocol Representation
• Protocol Definition
• Payload Types
• Header Attributes & Methods
• VDI Requirement Areas
• Other Standards Development Organizations (SDO)
• Roadmap – Next steps
List of Acronyms

• IETF – Internet Engineering Task Force
• CSP – Cloud Service Provider
• VDI – Virtual Desktop Infrastructure
• VDC – Virtual Desktop Client
• VDA – Virtual Desktop Agent
• VM – Virtual Machine
• DC – Data Center

• CSA – Cloud Security Alliance
• SDO – Standards Development Organizations
• PCI – Payment Card Industry
• DSS – Data Security Standards
• SOX – Sarbanes Oxley
Purpose

The purpose of the Virtual Desktop Infrastructure (VDI) Working Group: Protocol & Profiles
Protocol Representation

- Application Protocol Header
  - GRC Header
    - Non Functional Header
      - Functional Header
        - Application Specific Payload
Protocol Definition

- Attributes & Methods corresponding to the following:
  - Application Protocol Header – HTTP/SMTP/VOIP/IPTV
  - GRC Header - SOX, PCI DSS
  - Non Functional Header – business continuity (network, reliability, availability & performance)
  - Functional Header – REST/SOAP, cloud security attributes
  - Payload – POST Data/AVI/MPEG
Payload Types

Live
- Web Application Form Data (Structured text/html)
- Image
- Voice
- Video
- Attachments (unstructured/MIME data types)
- Unstructured data

Archive
- Structured Data (Database, etc)
- Files
  - Data – PDF, DOC, Excel, etc
  - Image - JPEG, GIF, PNG, etc
  - Voice archive – MP-3, etc
  - Video Archive – MPEG-4, MPEG-2, MJPEG, AVCHD, etc
- Unstructured data
# Header Attributes & Methods (Sampling)

<table>
<thead>
<tr>
<th>Client Attributes</th>
<th>Host Attributes</th>
<th>Data Attributes</th>
<th>Network Channel Attributes</th>
<th>Facility Attributes</th>
</tr>
</thead>
<tbody>
<tr>
<td>URL</td>
<td>Protocol attributes – referrer, etc</td>
<td>Encrypted or Not</td>
<td>Secure Channel</td>
<td>Personnel Access Control</td>
</tr>
<tr>
<td>Session Id</td>
<td>Hostname (virtual or hard) &amp; port</td>
<td>Location</td>
<td>DMZ or Core</td>
<td>Data center Servers RFIDs</td>
</tr>
<tr>
<td>Page Id</td>
<td>Context root</td>
<td>Sanitized or Not</td>
<td>Bandwidth Available</td>
<td>Data center room cameras</td>
</tr>
<tr>
<td>User Identity</td>
<td>Application Context</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Cookie Enabled</td>
<td>Session Context</td>
<td></td>
<td>Connection Type</td>
<td></td>
</tr>
<tr>
<td>Http Only &amp; Secure Flag</td>
<td>Page Context</td>
<td></td>
<td>Route</td>
<td></td>
</tr>
<tr>
<td>Query parameters</td>
<td>Cluster, Load Balanced, Failover &amp; DR</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Consumer Id &amp; Location Id</strong></td>
<td><strong>Provider Id &amp; Resource Location Id</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Method Id</td>
<td>Server Configurations (Timeouts)</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Identity Management</th>
<th>I/O Data Validation</th>
<th>Safe Coding Practices</th>
<th>Safe Install &amp; Config Practices</th>
<th>Facility Management</th>
</tr>
</thead>
<tbody>
<tr>
<td>Multi-factor, Single-Sign on Federation, Authentication</td>
<td>Input Sanitization for SQL, LDAP, Header Injection</td>
<td>Encoding, Logging, etc</td>
<td>LDAP/AD config for multi-tenancy</td>
<td>Time of Day rules</td>
</tr>
<tr>
<td>Authorization</td>
<td>Encoding of output of javascript or HTML data</td>
<td></td>
<td>Database configuration for multi-tenancy</td>
<td>Access Controls</td>
</tr>
<tr>
<td>Auditing</td>
<td>Input Length Check to avoid overflows</td>
<td></td>
<td>VLAN for multi-tenancy</td>
<td></td>
</tr>
</tbody>
</table>

*Note: Do not assume all cloud resources are virtualized to support multi-tenancy*
VDI Requirement Areas

- VDC Personalization
- VDC to & fro VDA communication
- VDA profile resources management (across CSPs)
Other Standards Development Organizations (SDO)

- Cloud Security Alliance (CSA)
- VMWare’s DMTF – vCloud API & Open Virtualization Format (OVF)
- TM Forum’s Cloud Program
- Open Cloud Computing Interface Working Group
- Amazon EC2 API
- Sun’s Open Cloud API
- Rackspace API
- GoGrid API
- Trust Computing Group
- National Institute of Standards and Technology (NIST)
- OASIS
- SNIA Security Forum
Roadmap – Next Steps

• Thoughts & Ideas for next steps