Security Benchmarks

Terry Sherald
sheraldt@ritchie.disa.mil
717-267-9969
11 June 2003
Where We Are

Building 1
Letterkenny Army Depot
Chambersburg

7/11th Mile

Skyline
(Eagle)
Falls Church
WHAT is a STIG?

• Security Technical Implementation Guide:
  – A Compendium of Security Regulations and Best Practices for Securing an Operating System or Application Software
  – A Guide for Information Security
  – Use is Mandated in by DISA Instruction 630-230-31
  – Authorized DODD 8500.1

• GOALS
  – Intrusion Avoidance
  – Intrusion Detection
  – Response and Recovery
  – Security Implementation Guidance
- Provides Standard, Secure environment for application development and operation
- Does not replace requirement for application security policy
- DISA is developing an Applications Developer Guide
STIG Lifecycle

- Draft STIG Distributed
- Technical Interchange Meetings (TIM)
- Final STIG
- Develop Checklist
- Draft STIG Distributed
- Technology Research
- Develop Assessment Tools
- New STIG

Unclassified
**DISA Security Technical Implementation Guides (STIGs)**

**NETWORK/PERIMETER**

<table>
<thead>
<tr>
<th>NIPRNet</th>
<th>Enclave</th>
<th>Network Infrastructure</th>
</tr>
</thead>
<tbody>
<tr>
<td>Wireless</td>
<td>DNS</td>
<td>Secure Remote Computing</td>
</tr>
</tbody>
</table>

**OPERATING SYSTEM**

<table>
<thead>
<tr>
<th>OS 390 (MVS)</th>
<th>VM</th>
<th>LPAR</th>
</tr>
</thead>
<tbody>
<tr>
<td>Unisys</td>
<td>Tandem UNIX</td>
<td></td>
</tr>
<tr>
<td>Novell</td>
<td>Win NT (NSA)</td>
<td>Win 2K (NSA)</td>
</tr>
<tr>
<td>Win XP</td>
<td>Win NT/2K Addendum</td>
<td></td>
</tr>
</tbody>
</table>

**APPLICATION**

<table>
<thead>
<tr>
<th>Database</th>
<th>Web Services</th>
</tr>
</thead>
<tbody>
<tr>
<td>Desktop Applications</td>
<td></td>
</tr>
</tbody>
</table>

**USER**

Security Handbook

**AVAILABLE AT THE FOLLOWING WEB SITES**

- https://iase.disa.mil
- http://iase.disa.smil.mil
- http://guides.ritchie.disa.mil (Uses PKI cert or userid/password)
  
  Contact FSO Support Desk for access – fso_spt@ritchie.disa.mil

Unclassified
Draft/Future STIGs

• Current Drafts
  – Network Infrastructure
  – OS/390
  – Logical Partition (LPAR)
  – Virtual Machine (VM)
  – Tandem
  – UNISYS
  – Wireless
  – Database
  – Web
  – Enclave

• New STIGs in FY03
  – Voice Over IP (VOIP)
  – Optical
  – Biometrics
  – MAC
DISA Implementation

- Gold Standard
  - Applied to STIGs
  - Checklist
  - Scripts
  - Tools
- Gold Standard Minimum Rqmt for Connection
- C&A Based on FULL STIG
- Gold Disk Tool
  - Gold Standard Prototypes
    - Windows 2000 and XP
    - Solaris
  - Production Gold Disk (FUTURE)
Issues

• Target Audiences (Home User, Corporate, etc.)

• Gold Standard vs. FSO Gold Standard
  – Specific DOD Issues

• Scoring Issues from CIS Tool
  – Example: /etc/inetd.conf (Tool – no, STIG – yes)
  – What is a Vulnerability?

• Application Specific Issues
  – Interoperability between Operating System and Application (i.e., Oracle) Security Settings

• Testing of Benchmark
  – Difficult to Find Participants
Lessons Learned

• Settings still Break Things
• Not enough time to be as active as needed
  – Raising issues to the Benchmark (CIS)
• Contingencies for Specific Settings
Benefits

- **Vendor involvement**
  - Success Story - Microsoft Security Guide
  - Providing Direction to Vendors

- **STIG Improvements**
  - Documentation of Setting Keystroke fixes
  - Technical Resources and Expertise

- **Windows**
  - Starting to Focus on Non-native Environments vs. Native W2K