



Argus Systems Group(www.argus-systems.com) PitBull.comPack™

Executive Summary

The SEWPSC is a SEWP-sponsored facility that evaluates IT security products and components of commercial off-the-shelf (COTS) products to determine their usability as well as to assess the vendor claims. The SEWPSC demonstrates security features of commercial, public domain, and Government products that can support dependable security architectures. The testing outlined in this document was conducted to assess ARGUS SYSTEMS GROUP, Inc. claims of performance, technical security, functionality and interoperability for their PitBull Foundation™ and PitBull.comPack™ product in an environment modeling typical user architecture(s), NASA constructed an environment reflecting their own other typical environments.

During the period 23-25 August 00, the staff of NASA's SEWPSC tested PitBull.comPack, a high-security web/transaction software product for Sun Microsystems' Solaris 2.7 servers (NOTE: Versions of this product are also available for IBM's AIX 4.33). The testing was conducted under the auspices of DoD's Security-Proof of Concept-Keystone (SPOCK) consortium and was supported by members of the SPOCK management office as well as the vendor, Argus Systems Group, Inc. The purpose of this *initial* report is to provide the results of this test relative to whether or not the vendor-provided product claims were successfully demonstrated to the NASA/SEWP's satisfaction.

Representatives from NASA SEWPSC, DoD, and Argus Systems Group conducted an extensive array of tests against 10 vendor-provided and 3 NASA-requested product claims (see result matrix on the following page). On all claims tested, it was concluded that PitBull.comPack successfully demonstrated the product's ability to meet all claims tested (See Preliminary Result Matrix). Claim 8a was the only claim not tested due to the lack, at NASA, of a PAM-compliant biometric authentication product. Interested government agencies should note that the Argus product is now available via the NASA SEWP II procurement vehicle. Additional information on the product, the testing process, and the testing methodology can be found within the *PitBull.comPack SPOCK Claims Package* dated August 00 and the *Argus White Paper: PitBull Security-The solution Set for Secure Systems*, dated July 00. see www.coact.com for points of contact and information on the NSA/V2 sponsored SPOCK consortium. SPOCK is scheduled to conduct additional testing on the: PitBull.comPack Product and compile a summarized SPOCK report containing details and combined input of the SEWPSC and follow-on exercises.

The complete SEWPSC Argus report is available to authorized US government employees. To request a copy, send an email to: sewpsc_reports@sewp.nasa.gov. Please include a contact name, Agency name, phone number, and fax number in your email.

PRELIMINARY RESULTS Matrix	SUBSTANTIATED	NOT SUBSTANTIATED	TESTED
<p>Claim 1: PitBull.comPack 2.1 installs onto operational Solaris 2.7 (recommended release date of 8/99 or later) hosts running standard applications without requiring the removal/reintegration of the existing operating system or application software.</p>	X		
<p>Claim 2: When users of Argus systems install applications conforming to commercial Solaris API(s), these applications will function in the same manner that they would on standard Solaris 7.2.Internet-centric</p>	X		
<p>Claim 3: PitBull.comPack will provide a secure interface between unauthorized users and sensitive internal applications and systems.In so doing, it can also segregate multiple networks and create virtual networks.</p>	X		
<p>Claim 4: PitBull.comPack enforces the integrity of network transactions through separation of duties and the two-person rule (See 4a and 4b):4.Transparent/Dependable</p>			

4a: PitBull.comPack provides a mechanism for controlling user authorizations of both users and administrators via operating system-enforced security.	X		
4b: Enforces Two-Person Rule and Administrative Roles of Information System Security Officer, System Administrator, and System Operator	X		
5. Protects Web Pages against unauthorized modification	X		
6. Provides operating system enforced Mandatory Access Controls (MAC) (to data, applications, network devices, and/or users)	X		
7. Least Privilege is enforced upon users and applications	X		
8. Flexible and configurable security to include (See 8a and 8b):			
8a: Enhanced password/authentication mechanisms utilizing Pluggable Authentication Modules (PAM).			X
8b: Secure Remote SSH Administration	X		
9. Value Added (NASA Originated) Demonstrations (See 9a and 9b):			

<p>9a: Monitors and records subsystem security-relevant events.</p>	<p>X</p>		
<p>9b: Provides threat protection via compartmentalization (labeling)/safeguards</p>	<p>X</p>		
<p>9c. Examine Command Center GUI for applicability to system security administration functions</p>	<p>X</p>		