

2013 DHS S&T/DoD ASD (R&E)  
CYBER SECURITY SBIR WORKSHOP

# XEBHRA: A Virtualized Platform for Cross Domain Information Sharing

Adventium Labs  
Charles N. Payne, Jr.

*July 23, 2013*



Homeland  
Security

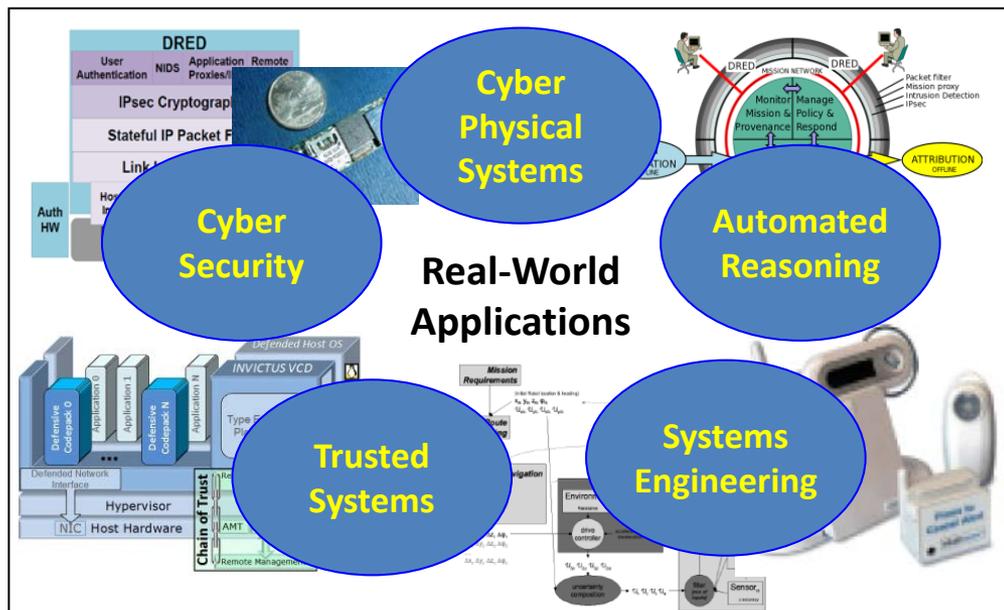
Science and Technology



# Company Profile



- Scientist-owned small business, founded 2002
- Commercial and government contract research
- **Technical Staff:** Ph.D.: 50%, MS: 30%, BS: 20%
- **Fields:** Computer Science, Mathematics, Electrical Engineering, Psychology
- **Career patents:** 25 issued (3 AL), 33 pending (5 AL)
- **Publications:** 300+
- **2012 DoD commercialization score:** 95 (up from 90 in 2011)



## Selected Transition Successes:

- SAFEbus® for Boeing 777 and C5-AMP Integrated Modular Avionics
- Guidant LATITUDE wireless medical devices
- 3Com Embedded Firewall
- DTOS (Distributed Trusted Operating System) – foundation of SE Linux
- DEOS Real-Time Operating System

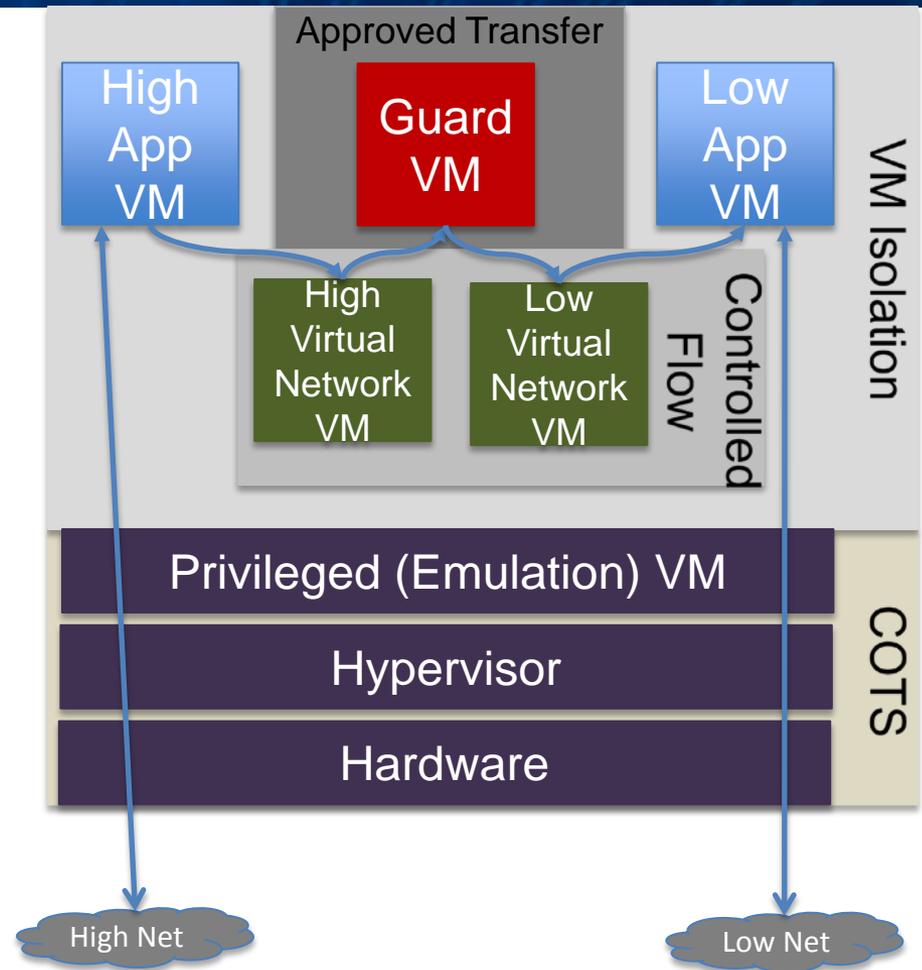
# Customer Need

- DoD and IC missions share information across multiple information security domains, using a certified guard to approve the transfer between domains.
- Despite the push for enterprise cross domain services, some missions require a locally managed guard.
- Currently a guard must be deployed on a separate physical host.
- Successful transfer requires at least three physical computers, one for each domain and one for the guard.
- Resource constrained environments (e.g., submarine, airplane, tank) are burdened by the higher Size, Weight and Power (SWaP) incurred.

**Lower SWaP for cross domain transfer in resource constrained environments.**

# Approach

- Co-locate the guard and **cross domain applications** as virtual machines (VMs) on the same physical hardware.
  - Cross domain transfer occurs locally -- without going through the physical network.
- Leverage **commercially available virtualization technologies** that offer strong assurances of VM isolation.
- Use already **certified guards** to approve information transfers.
- **Key innovation:** Use **virtual networks**, operating in their own isolated VMs, to force information flow between domains through the guard.



**The XEBRHA platform enforces information flow through the guard.**

# Benefits

- XEBHRA is designed to be agnostic to the guard and cross domain application used.
  - XEBHRA scales to support more domains and guards.
- The XEBHRA prototype exceeded expectations.
  - Installed unmodified Radiant Mercury guard.
  - Reduced SWaP 3-to-1 over physical host deployment.
  - Achieved end-to-end transfers (using null guard) comparable to 1 Gbps Ethernet, with < 1% overhead.
- XEBHRA protects the guard from direct attack from the physical networks.

**The XEBHRA platform reduces SWaP by at least 3-to-1 and uses existing guards.**

# Current Status

- Phase 2 SBIR completed in August 2011:
  - Demonstrated prototype for an operationally relevant cross domain application associated with a Navy Program of Record (PoR); briefed Navy and SPAWAR personnel.
  - Exhibited prototype at conference sponsored by the Unified Cross Domain Management Office (UCDMO).
- Migrated key portions to the Citrix XenClient XT hypervisor.
  - XenClient XT is also the hypervisor for the TSABI certified AFRL SecureView workstation (SABI underway).
  - Adventium has on-going collaboration with Citrix to build other information security appliances for XenClient XT.
- Selected for Navy RIF funding in 2012 but became a victim of budget cuts.
  - Defined certification plan for XEBHRA.
- Briefings for other Navy and Air Force PoRs have generated positive responses.

# Next Steps

- Identify funding to complete port of XEBHRA to Citrix XenClient XT.
- Identify PoR to sponsor XEBHRA certification (possibly using Phase IIB).
  - UCDMO recommended certifying XEBHRA as an alternate hardware platform for the guard.
  - The initial certification is the biggest hurdle.

# Contact Information

- Technical: Charles N. Payne, Jr.  
[charles.payne@adventiumlabs.com](mailto:charles.payne@adventiumlabs.com)  
(612) 817-2525
- Business Development: Dr. Lindsey Hillesheim  
[lindsey.hillesheim@adventiumlabs.com](mailto:lindsey.hillesheim@adventiumlabs.com)  
(612) 481-0533

Acknowledgments: This work was funded by the Office of the Secretary of Defense (OSD)/Navy SBIR program under OSD07-I11. Program technical direction was provided by the Naval Research Laboratory.

Disclaimer: The views and conclusions contained herein are those of the authors and should not be interpreted as representing the official policies, either expressed or implied, of the Naval Research Laboratory, the Office of the Secretary of Defense, or the U.S. Government.