DISTRIBUTION STATEMENT A. Approved for Public Release;
Distribution Unlimited; 88ABW-2009-3476, 31 July 2009

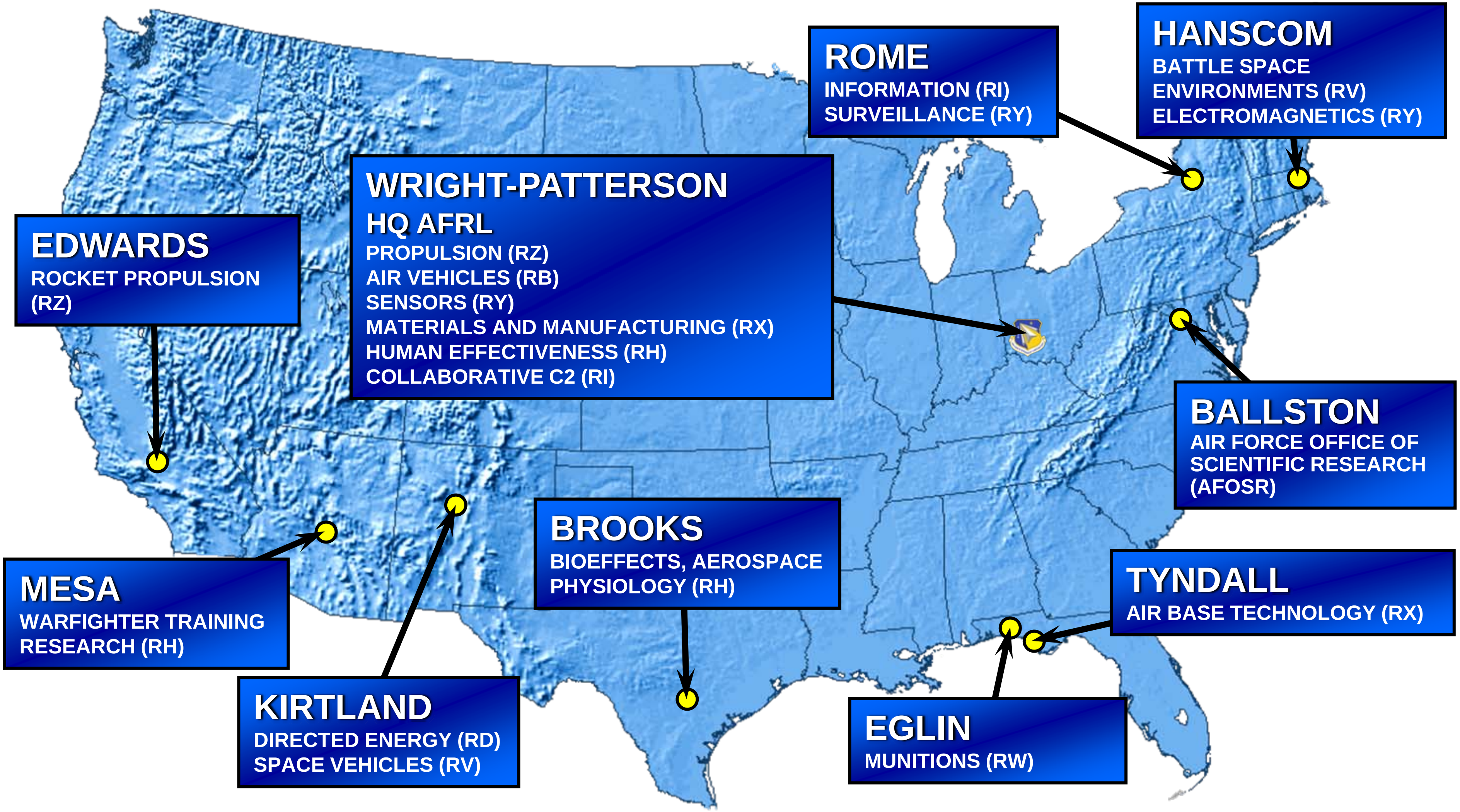
Air Force Research Laboratory, The Information Directorate and Layered Assurance

Steven L. Drager
Computing technology Applications Branch (AFRL/RITB)
Advanced Computing Division (AFRL/RIT)
Information Directorate (AFRL/RI)
Air Force Research Laboratory

Air Force Research Laboratory (AFRL) Mission

Leading **the discovery, development, and integration of affordable warfighting technologies for our air, space and cyberspace force.**

Major AFRL Facilities



ROME
INFORMATION (RI)
SURVEILLANCE (RY)

HANSCOM
BATTLE SPACE ENVIRONMENTS (RV)
ELECTROMAGNETICS (RY)

WRIGHT-PATTERSON
HQ AFRL
PROPULSION (RZ)
AIR VEHICLES (RB)
SENSORS (RY)
MATERIALS AND MANUFACTURING (RX)
HUMAN EFFECTIVENESS (RH)
COLLABORATIVE C2 (RI)

EDWARDS
ROCKET PROPULSION (RZ)

BALLSTON
AIR FORCE OFFICE OF SCIENTIFIC RESEARCH (AFOSR)

BROOKS
BIOEFFECTS, AEROSPACE PHYSIOLOGY (RH)

MESA
WARFIGHTER TRAINING RESEARCH (RH)

TYNDALL
AIR BASE TECHNOLOGY (RX)

KIRTLAND
DIRECTED ENERGY (RD)
SPACE VEHICLES (RV)

EGLIN
MUNITIONS (RW)

DISTRIBUTION STATEMENT A. Approved for Public Release; Distribution Unlimited; 88ABW-2009-3476, 31 July 2009

AFRL Organization

Commander (CC)
Maj Gen Curtis Bedke

Executive Director (CA)
Mr Joe Sciabica

Vice Commander (CV)
Col David Glade II

Chief Technology Officer (CZ)
Dr Mike Kuliasha

AFOSR

Propulsion
(RZ)

Directed Energy
(RD)

Information
(RI)

711 Human
Performance Wing

Munitions
(RW)

Sensors
(RY)

Space Vehicles
(RV)

Materials &
Manufacturing (RX)

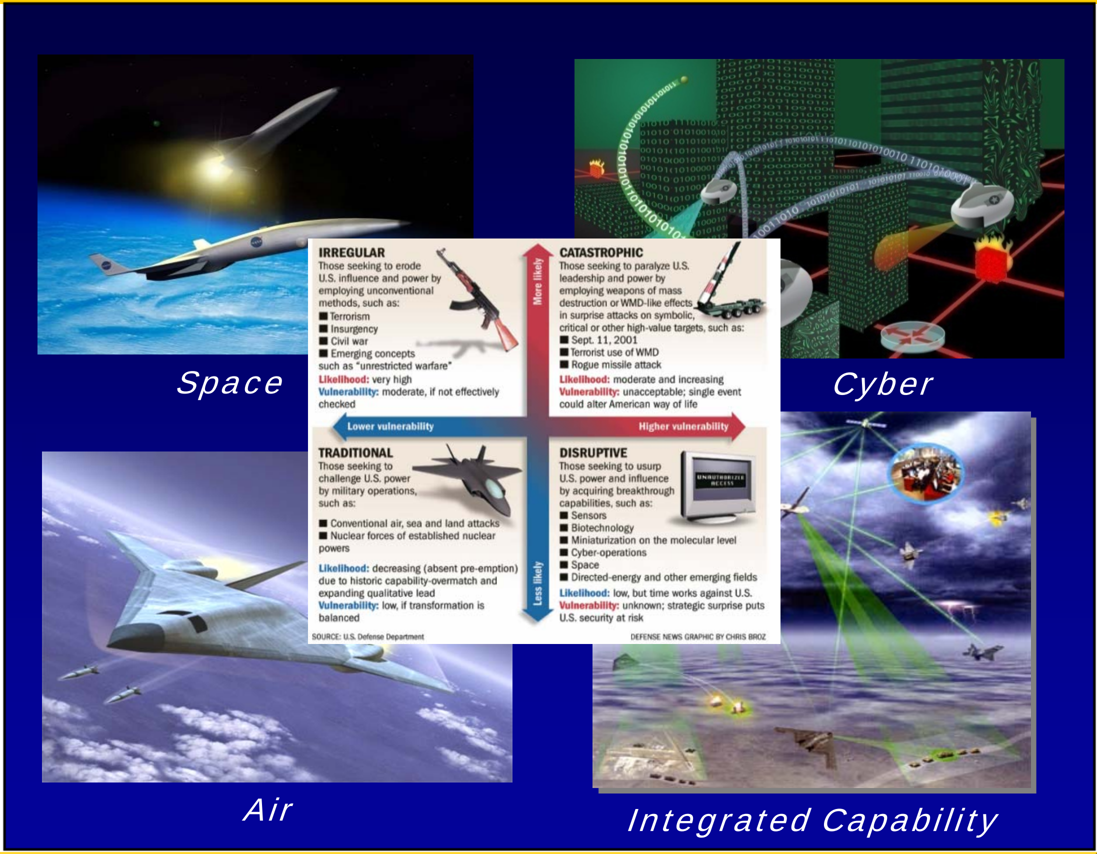
Air Vehicles
(RB)

Human
Effectiveness
(RH)

AFRL’s Focused Long Term Challenges

Delivering the Air Force S&T Vision Through Leadership, Discovery, Innovation, and Integration.

1. **Anticipatory Command, Control & Intelligence (C2I)**
2. **Unprecedented Proactive Intelligence, Surveillance & Reconnaissance (ISR)**
3. **Dominant Difficult Surface Target Engagement/Defeat**
4. **Persistent & Responsive Precision Engagement**
5. **Assured Operations in High Threat Environments**
6. **Dominant Offensive Cyber Engagement**
7. **On-demand Theater Force Projection, Anywhere**
8. **Affordable Mission Generation & Sustainment**



IRREGULAR
Those seeking to erode U.S. influence and power by employing unconventional methods, such as:
- Terrorism
- Insurgency
- Civil war
- Emerging concepts such as “unrestricted warfare”

Likelihood: very high
Vulnerability: moderate, if not effectively checked

CATASTROPHIC
Those seeking to paralyze U.S. leadership and power by employing weapons of mass destruction or WMD-like effects in surprise attacks on symbolic, critical or other high-value targets, such as:
- Sept. 11, 2001
- Terrorist use of WMD
- Rogue missile attack

Likelihood: moderate and increasing
Vulnerability: unacceptable; single event could alter American way of life

TRADITIONAL
Those seeking to challenge U.S. power by military operations, such as:
- Conventional air, sea and land attacks
- Nuclear forces of established nuclear powers

Likelihood: decreasing (absent pre-emption) due to historic capability-overmatch and expanding qualitative lead
Vulnerability: low, if transformation is balanced

DISRUPTIVE
Those seeking to usurp U.S. power and influence by acquiring breakthrough capabilities, such as:
- Sensors
- Biotechnology
- Miniaturization on the molecular level
- Cyber-operations
- Space
- Directed-energy and other emerging fields

Likelihood: low, but time works against U.S.
Vulnerability: unknown; strategic surprise puts U.S. security at risk

SOURCE: U.S. Defense Department

DEFENSE NEWS GRAPHIC BY CHRIS BROZ

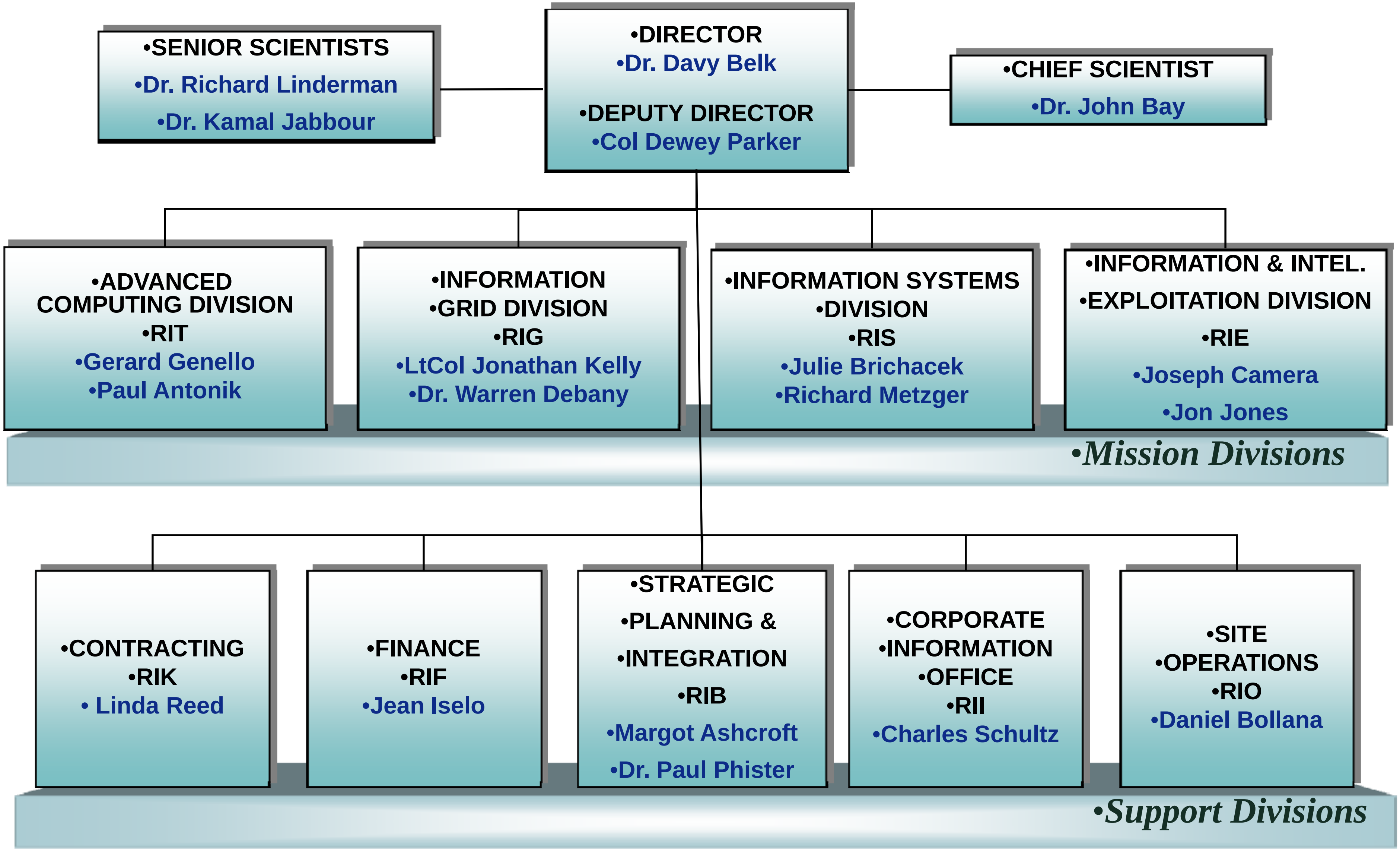
AFRL Technology Supporting Tomorrow’s Warfighter

Information Directorate

Mission: To lead the discovery, development, and integration of affordable warfighting information technologies for our air, space and cyber force.

Vision: To defend America by unleashing the power of innovative information science and technology to anticipate, find, fix, track, target, engage, and assess anything, anytime, anywhere.

Information Directorate Organization



•SENIOR SCIENTISTS

•Dr. Richard Linderman

•Dr. Kamal Jabbour

•DIRECTOR
•Dr. Davy Belk

•DEPUTY DIRECTOR
•Col Dewey Parker

•CHIEF SCIENTIST

•Dr. John Bay

•ADVANCED COMPUTING DIVISION
•RIT
•Gerard Genello
•Paul Antonik

•INFORMATION
•GRID DIVISION
•RIG
•LtCol Jonathan Kelly
•Dr. Warren Debany

•INFORMATION SYSTEMS
•DIVISION
•RIS
•Julie Brichacek
•Richard Metzger

•INFORMATION & INTEL.

•EXPLOITATION DIVISION

•RIE

•Joseph Camera

•Jon Jones

•Mission Divisions

•CONTRACTING
•RIK
• Linda Reed

•FINANCE
•RIF
•Jean Iselo

•STRATEGIC

•PLANNING &

•INTEGRATION

•RIB

•Margot Ashcroft

•Dr. Paul Phister

•CORPORATE
•INFORMATION
•OFFICE
•RII
•Charles Schultz

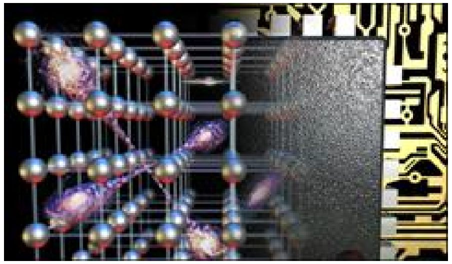
•SITE
•OPERATIONS
•RIO
•Daniel Bollana

•Support Divisions

Information Directorate
Core Technical Competencies (CTCs)

Information Exploitation

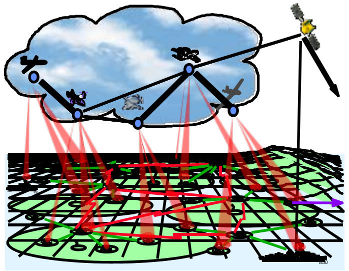
Information Fusion & Understanding



Advanced Computing Architectures

Cyber Operations

Information Management



Connectivity

Command & Control

DISTRIBUTION STATEMENT A. Approved for Public Release; Distribution Unlimited; 88ABW-2009-3476, 31 July 2009

Why Trusted Computing?

- World Economy
  - Both hardware and software are researched, developed and manufactured with unknown provenance
- Sources of Vulnerabilities
  - Used to be the Operating System (e.g. Windows)
  - Now they are Everywhere
    - Web vulnerabilities have overcome system vulnerabilities
    - Adobe just announced another critical vulnerabilty
    - Circumvention of Intel’s tBoot

Who do we need to trust today?

- Hardware
  - CPU manufacturers (Intel?, AMD?)
  - Motherboard manufacturers (ASUS?)
  - BIOS manufacturers (Award?, Phoenix?)
- Operating systems
  - Microsoft?
  - Redhat?
  - Open source community?

In HAC we do…

- not research Trojan Circuits and protections against them. DARPA
  - assume that a “trusted foundry” exists
- not research Anti-Tamper technologies
  - assume that products can be “protected”
- research high assurance computing issues
  - Low level computer architectures
  - Operating Systems
  - Hardware / Software co-solutions
  - Software
    - Leverage from Software Producibility
- not research “applications” although we do take a systems engineering approach

DISTRIBUTION STATEMENT A. Approved for Public Release; Distribution Unlimited; 88ABW-2009-3476, 31 July 2009

How we (AFRL) are getting there.

Research

New

- Costly
- Gov’t pays
- Long lead time
- As high-assurance as needed

Add-on

- Cost effective
- Shared costs
- Near term
- Limited by the “base”

DISTRIBUTION STATEMENT A. Approved for Public Release; Distribution Unlimited; 88ABW-2009-3476, 31 July 2009

Example: Architectures for Trusted Computing Bases

Single/Multi Core Many Core FPGA

- **If we can integrate a “trusted module” (like a TPM, but not necessarily a TPM) into modern processors …**
  - What will it look like?
  - What kind of function(s) will it perform?
  - How will these changes affect the rest of the system?
  - How many will there be?
  - How will this processor be different?
  - How can we build it for high assurance?

Example: Architectures for Trusted Computing Bases

Single/Multi Core | Many Core | FPGA

- Tomorrow’s Many Core processors will likely be partially reconfigurable (poly-morphic?) to support multiple concurrent applications. If there is such a thing as a trusted module, then
  - What will it look like? Especially if it is heavily SWaP contrained?
  - What kind of function(s) will it perform?
  - How will these changes affect the rest of the system?
  - How many will there be and how will they be organized?
  - How can we build it for high assurance?

Example: Architectures for Trusted Computing Bases

Single/Multi Core | Many Core | **FPGA**

- **One of the major areas of concern of modern computer systems is the TPM being essentially a “slave” to the CPU. Can we make the TPM the “master” instead? And if so …**
  - **What will this trusted module look like?**
  - **Will this really make legacy systems “trustworthy”?**
  - **Can reconfigurable systems (FPGAs) be trusted?**

Opportunities

Commercial

- Trusted eXecution Technologies
- Virtualization Extensions
- Bleeding-edge processors

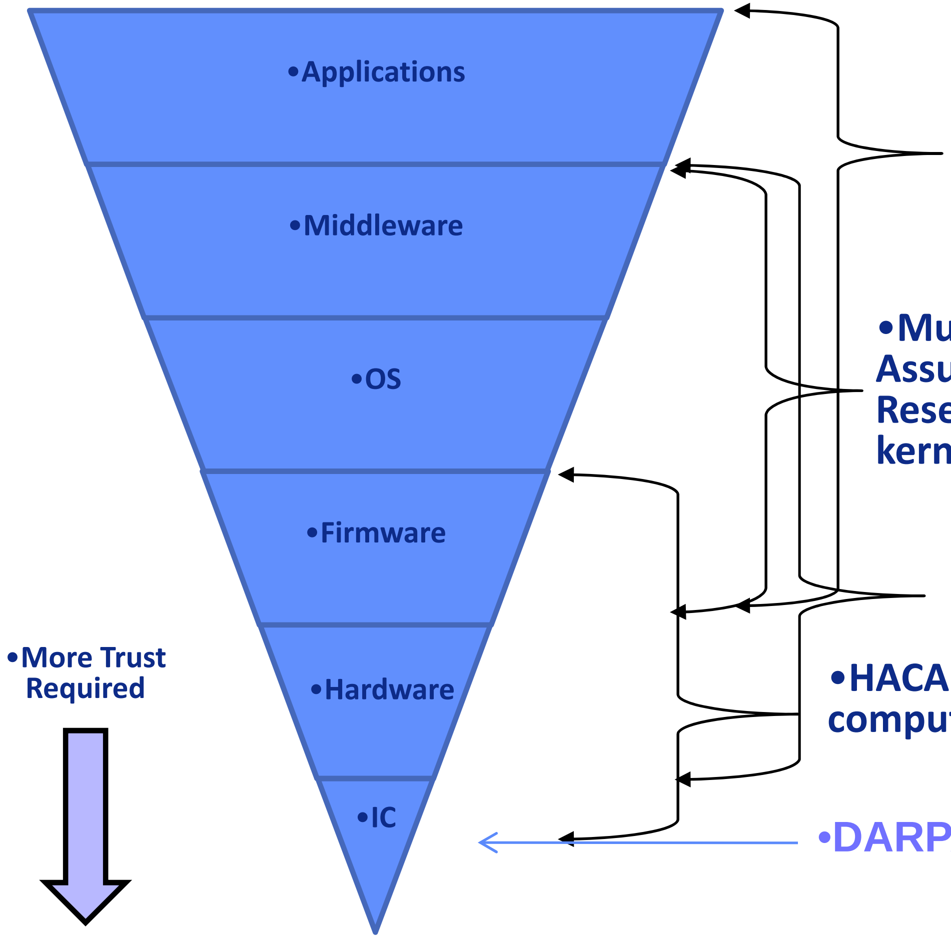
Air Force Research Lab

- Roots of Trust
- Virtual Cybercraft
- Architectures for Trusted Computing Bases

Capabilities Overview

- Novel high performance computing resources cyber testing and computations – Computational Science and Engineering: Emulab
- Eliminate software vulnerabilities before they manifest by increasing the “correctness” of code while reducing the cost of producing software – Software Intensive Systems Producibility: SPRUCE
- Pervasive low-level software (operating systems and hypervisors) protection that integrate state of the art hardware and software solutions – High Assurance Computing: MILS and Secure Core
- Assured (trustworthy) computing platforms of varying levels of assurance and trustworthiness – High Assurance Computing: High Assurance Computing Architectures

Cyber Related Research in ACA



- Software Producibility – Pervasive software program that seeks to improve the overall quality (includes security and trustworthiness) and producibility of software, from the firmware up to applications
- Multiple Independent Levels of Security / High Assurance Middleware for Embedded Systems – Research into separation kernels, secure micro-kernels and middleware.
- SecureCore – Integrated hardware/software solution for security
- HACA – The hardware basis for trustworthy computing systems
- DARPA TRUST Program

Support of Software Research for Cyberspace

- Poor software is the core of cyberspace security problems
- By increasing the "correctness" of our code we can eliminate potential vulnerabilities while increasing the detection of malicious code.
- The fewer unintentional bugs in software, the visibility of deliberate malware would be increased.*
- "…we have many commercial products that are riddled with logic flaws, which decrease the reliability of the target system, and the flaws are increasingly becoming the targets of system attacks using viruses and worms."**
- System Flaws = System Vulnerabilities

•* Defense Science Board Task Force on Mission Impact of Foreign Influence on DoD Software

•** John Gilligan – USAF CIO 2004

Solution?

- Revisit modern computer architectures
  - Start with current platforms and secure them (SecureCore and MILS)
  - Start with the core – processors and work our way out (ATCB)
- Focus on the concept of minimal trust
- Focus on modularity/extensibility
- Focus on security principles
- Focus on systems engineering

DISTRIBUTION STATEMENT A. Approved for Public Release; Distribution Unlimited; 88ABW-2009-3476, 31 July 2009

Brand New SBIR Topics

- **AF093-049: Self-Shielding Systems and Attack-Surface Mutation**
  - **Create a rapidly-shifting network architecture with agility and diversity to deter and prevent adversary reconnaissance and cyber attack planning activities and reduce effectiveness of attacks.**
- **AF093-053: Automatic Artificial Diversity for Virtual Machines**
  - **Apply artificial diversity and agility techniques in a virtual machine environment to thwart attacks.**

Conclusions

- We need to work closely with both local and national universities to adopt their new ideas and help educate their students on tomorrow’s trusted computing issues. – We are doing this!

- We need to work closely with industry to make trusted computing a reality. – We are also doing this!
  - This is especially true for leading chip manufacturers.

AFRL

THE AIR FORCE RESEARCH LABORATORY

LEAD | DISCOVER | DEVELOP | DELIVER