Combating Short- and Long-Term Cyber Threats

Stacey A. Dixon, Ph.D. | Deputy Director

Intelligence Advanced Research Projects Activity

Office of the Director of National Intelligence

I A R P A

BE THE FUTURE

25 October 2017

IARPA Partners & Customers: The Intelligence Community

IARPA Mission

IARPA envisions and leads *high-risk, high-payoff research* that delivers innovative technology *for future overwhelming intelligence advantage*

- Our problems are **complex** and **multidisciplinary**
- We emphasize **technical excellence** & **technical truth**

IARPA Method

Bring the best minds to bear on our problems

- Full and open competition to the greatest possible extent
- World-class, rotational Program Managers

Define and execute research programs that:

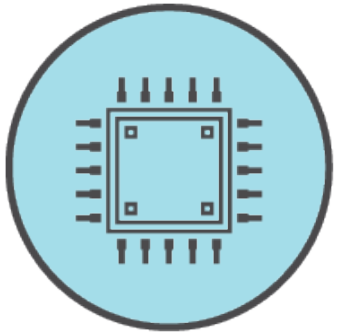
- Have goals that are clear, measureable, ambitious and credible
- Employ independent and rigorous Test & Evaluation
- Involve IC partners from start to finish
- Run from three to five years
- Publish peer-reviewed results and data, to the greatest possible extent
- Transition new capabilities to intelligence community partners

4 Core Research Thrusts

Analysis

Anticipatory Intelligence

Collection



Computing

Computing R&D

"Operate effectively in a globally interdependent and networked environment"

COMPUTATIONAL POWER

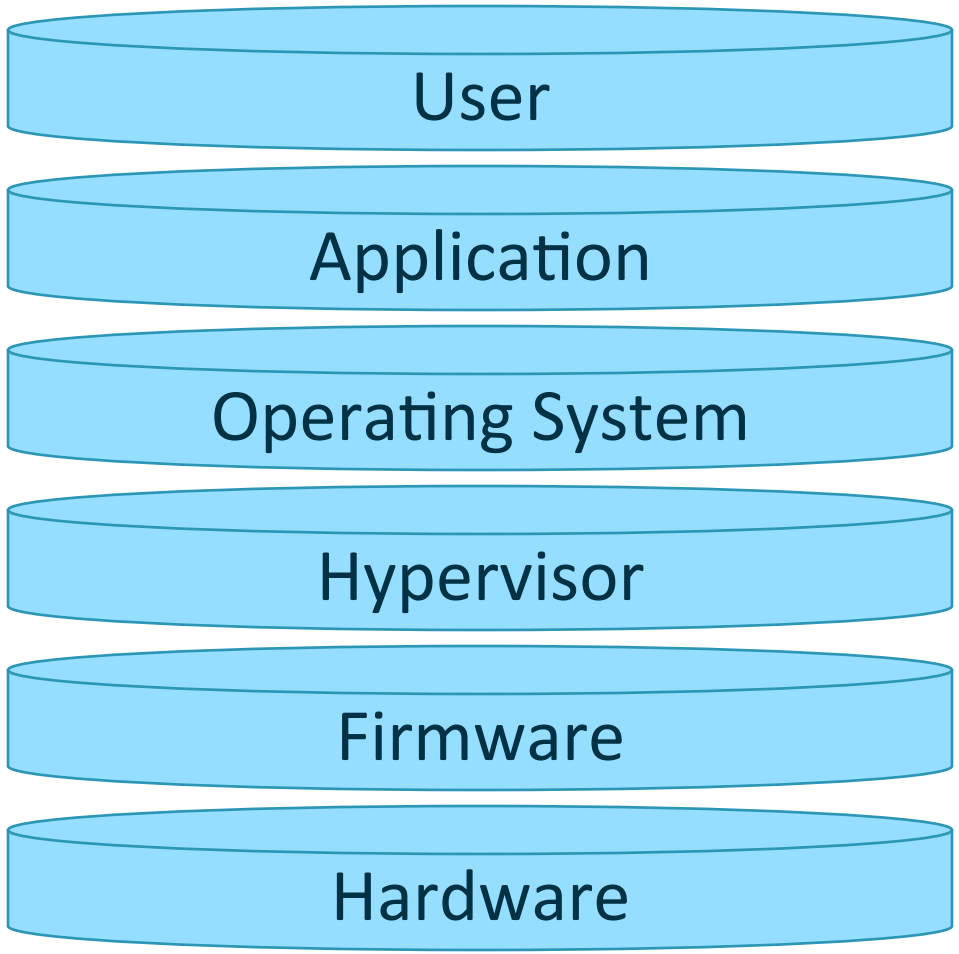
Revolutionary advances to solve problems intractable with today's computers

TRUSTWORTHY COMPONENTS

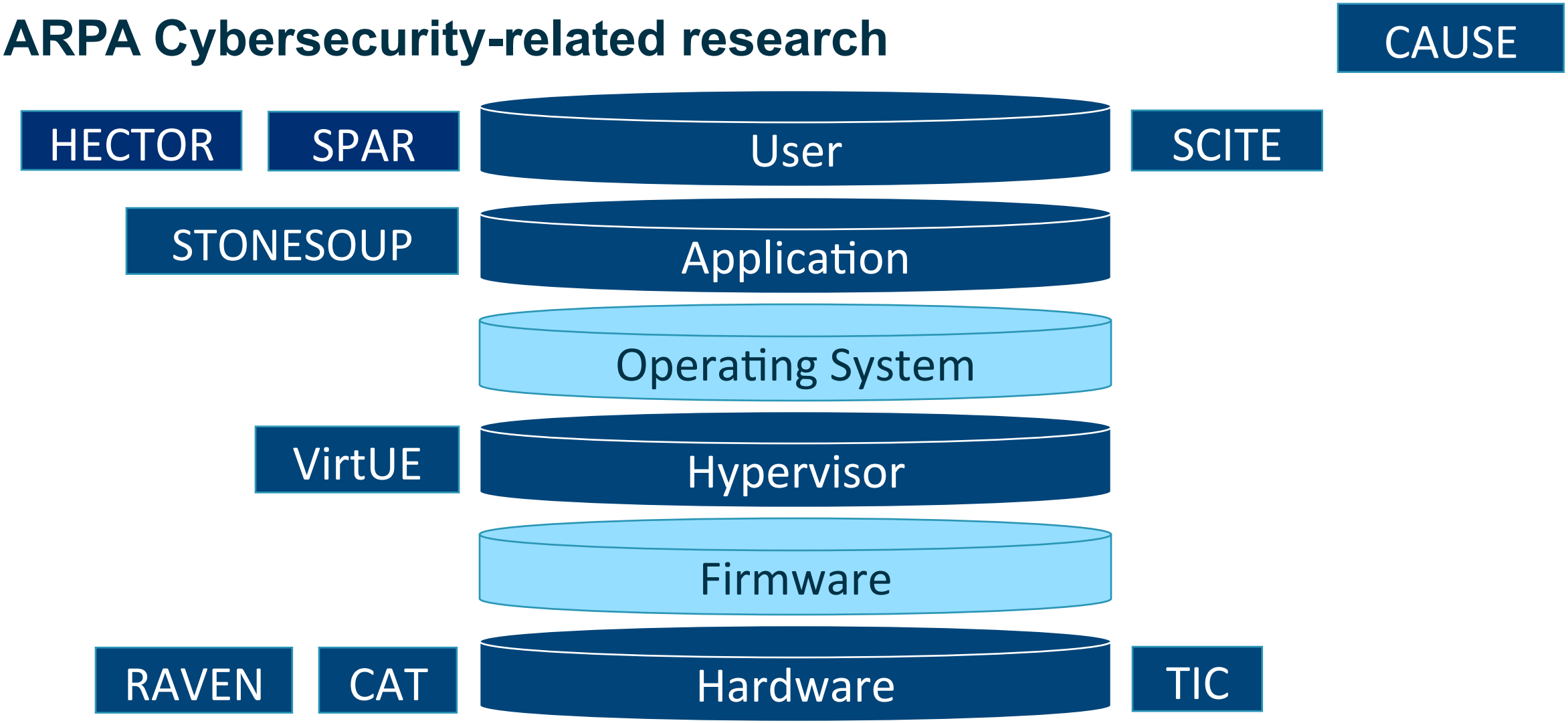
Gain the benefits of leading-edge hardware and software without compromising security

SAFE AND SECURE SYSTEMS

Protecting systems against cyber threats


User
Application
Operating System
Hypervisor
Firmware
Hardware

IARPA Cybersecurity-related research



Cyber-attack Automated Unconventional Sensor Environment (CAUSE)

- How can we forecast cyber-attack events, hours to weeks earlier than existing methods?

- CAUSE Program goals
  - Develop and validate unconventional multi-disciplinary sensor technology that will forecast cyber-attacks and complement existing advanced intrusion detection capabilities.

CAUSE Approach

Conventional Sensors:
Vulnerability, Attack Surface, etc.

Conventional Data Sources:
CVE,DNS logs, etc.

Traditional Technical Sensors

Publically Available Sensors

Cyber Attack Forecasting Model

Attack Forecast

Unconventional Sensors:
Intent, Sentiment, Political, Capability etc.

Unconventional Data Sources:
Social Media, Darkweb, etc.

Performer Innovation

Cyber Actor Models

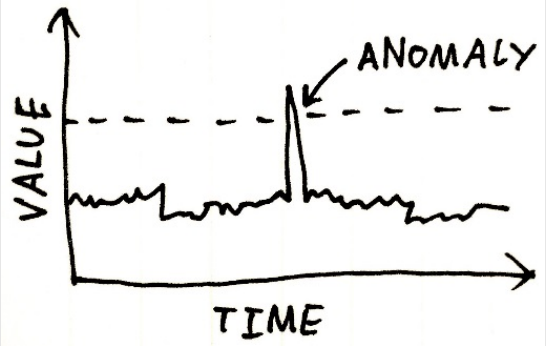
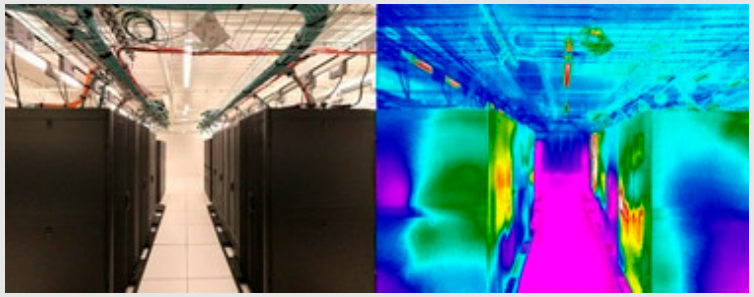
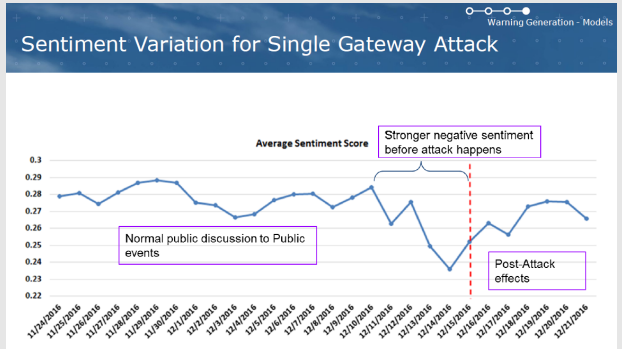
Non-State
State
Criminal

Early detection and forecasting of malicious cyber activity at scale

CAUSE Performer Modeling & Analytic Approaches

- Learning the spatio-temporal structure relating observable behaviors (e.g. social media interactions) with historical cyber-attack data
- Learning other features from sensor data (e.g., Darkweb posts) that are predictive of events
- Fusing not only predictions from multiple models, but signals from multiple sensors as well
- Training a translation model using a convolutional neural network (CNN) approach for feature extraction from websites in other languages

CAUSE Sensor Research

	CONVENTIONAL	UNCONVENTIONAL
INTERNAL	**Network Behavior Anomaly Detection** 	**Thermal Anomaly Detection** 
EXTERNAL	Are high frequency mentions of software vulnerabilities indicative of future cyber-attacks? **Vulnerability Mentions**	 **Social Media Sentiment Analysis**

CAUSE Program Challenges

- Challenge #1: Ground Truth
  - Event Types: a typology defining the relevant cyber-attack event space is necessary for predictive modeling and analytics
  - High Fidelity: accurate prediction of event details advances the state-of-the-art of cyber-attack forecasting and provides utility for deploying effective defensive measures
  - Lessons Learned: developing reliable data collection and encoding processes is paramount for executing a successful program

CAUSE Program Challenges

- Challenge #2: Transparency
  - Cybersecurity analysts are reluctant to adopt black box systems that fail to reveal the decision process and lack transparency
  - A program objective is to promote transparency by providing an Audit Trail capability to reveal the decision process and connect the dots
  - Narrative provides context about the warning from Audit Trail details

CAUSE Technical Challenges

- High Dimensional Data Sources
  - Pertinent data sources (e.g., social media, dark web, news) are inherently noisy and have high dimensionality
  - Key challenge to extract features and reduce dimensionality
- Sensor Research
  - Conventional and unconventional sensors rely on both internal (e.g., security appliance) and external data sources
  - Sensors measure multi-modal observable signals such as sentiment, outrage, and intent from multiple data sources
  - Key challenge to measure noisy signals indicative of cyber-attacks

Virtuous User Environment (VirtUE)

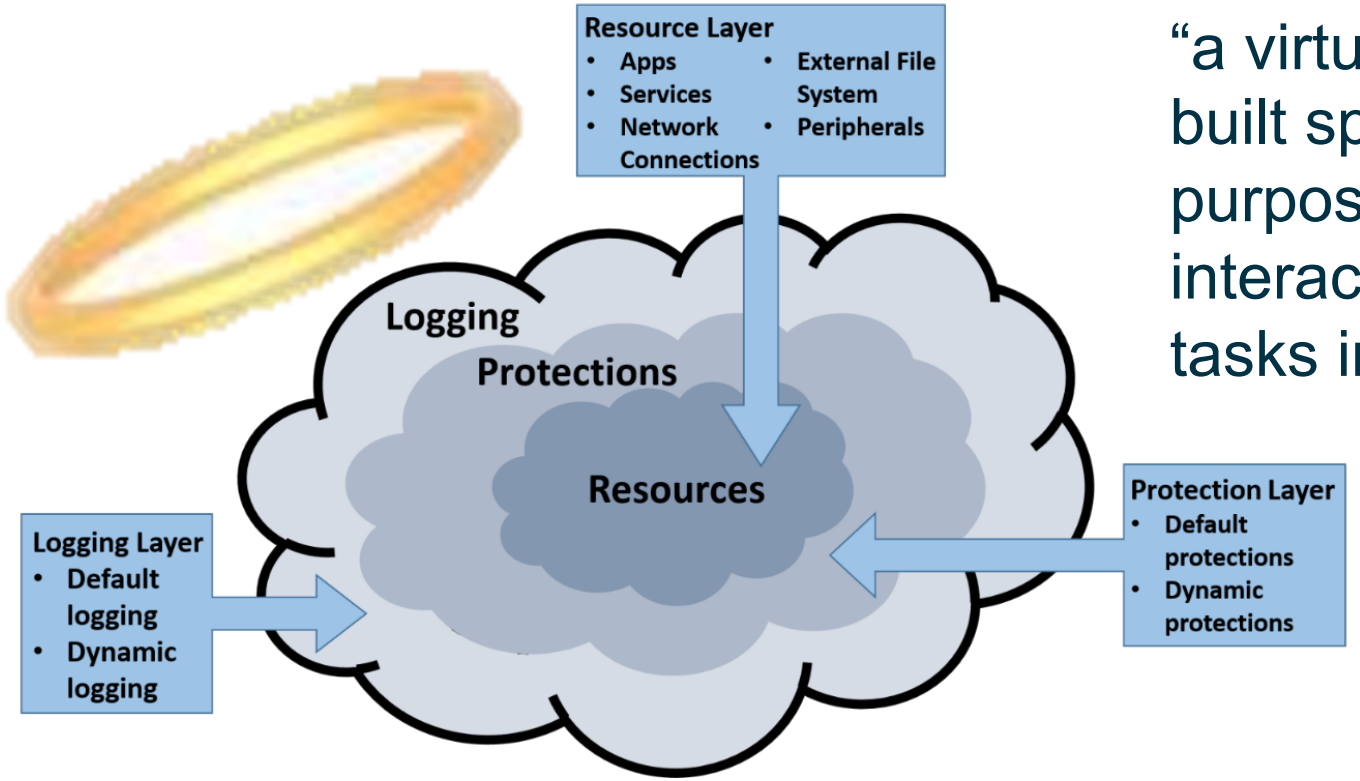
- How can we develop user environments that are more dynamic, secure, auditable, transferrable, and efficient than the current offerings provided by traditional physical workstations and commercial Virtual desktop infrastructure?

virtue

VirtUE Program Goals

- Use the technologies of the cloud to create a new user interface that mitigates user-based computer threats in the government's computing environment - "A better Virtual Desktop Infrastructure"
- Mitigate this Computer Security Conundrum:
  - Computer users are responsible for most of our current security incidents. Spear-Phishing, Malicious Web content, user carelessness or malice
  - Users need convenient access to computing resources to maintain productivity and achieve organizational goals

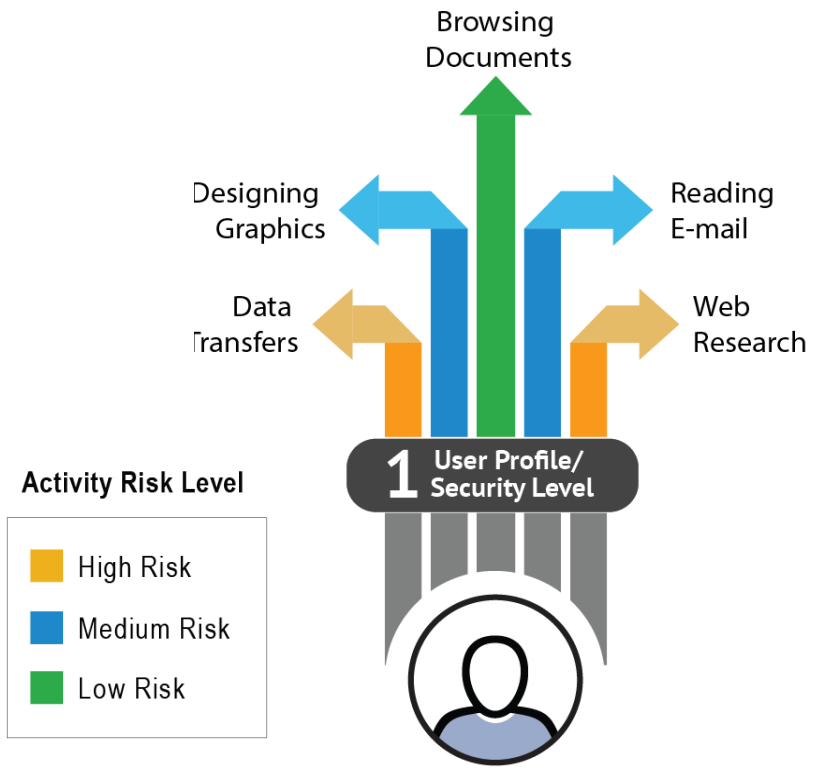
Build a Dynamic, Securable User Environment Using the Cloud – A "Virtue"



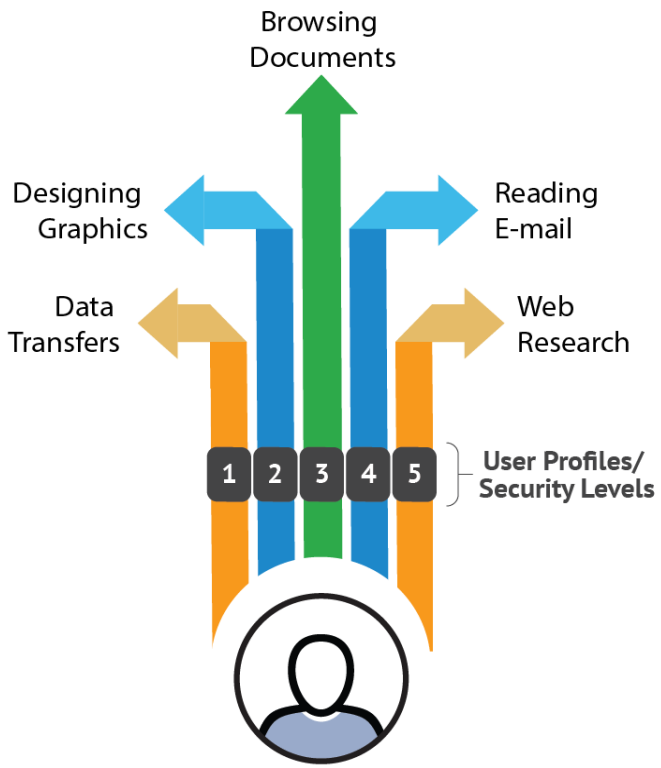
"a virtual appliance built specifically for the purpose of safe, user-interactive computing tasks in the cloud"

Redesign the Legacy User Environment Leveraging the Cloud

CURRENT MODEL



VIRTUE MODEL



Provide a Clever Presentation Interface Merging User's VirtUEs

User interacting with 6 virtues in one interface

Scientific advances to Continuous Insider Threat Evaluation (SCITE)

- How can we advance the science and practice of insider threat detection?

- Program Goals:
  - Model and forecast the performance of existing and proposed insider threat detection enterprises
  - Develop a new class of active indicators and associated automated detection tools
- Status: program in progress

Security and Privacy Assurance Research (SPAR)

- What do you do when a query is too sensitive to share, and bulk ingestion of the data raises privacy issues?

Client learns:

- Response
- Query policy
- Other record contents
- Other clients' queries

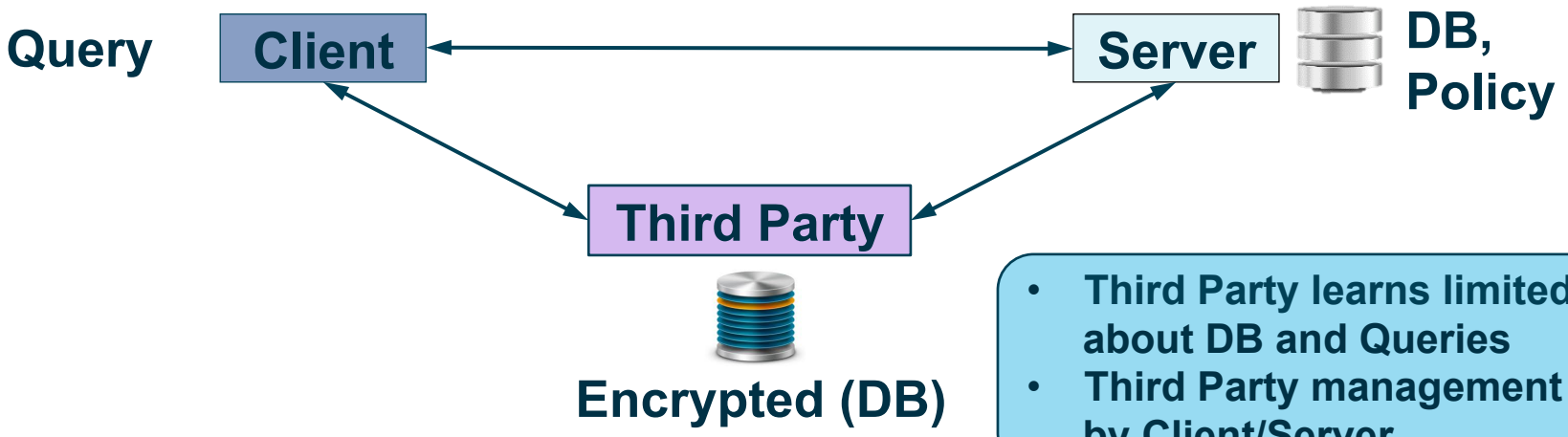
Server learns:

- Query structure
- Query contents
- Query response
- Cross-query trends

SPAR Program Goals

- Create systems that guarantee privacy while also maintaining certain security characteristics
- Gives assurance to a data owner that only relevant information is shared
- Supports a practical set of query types and scales to realistic database sizes
- Enables collaboration between non-traditional/occasional partners, and administration without access to content

SPAR Sharing Architecture



- Third Party learns limited information about DB and Queries
- Third Party management jointly decided by Client/Server

Client learns:

- Response
- Query policy
- Other record contents
- Other clients' queries

Third party learns:

- Query structure
- Cross-query trends
- # of records returned
- Query contents
- Record contents

Server learns:

- Query structure
- Query contents
- Query response
- Cross-query trends

Homomorphic Encryption Computing Techniques with Overhead Reduction (HECTOR)

- Challenge: To **balance** the needs of **policy compliance with** providing **access** to data needed to protect national security.

- Goal: Develop a comprehensive set of cryptographic tools, programming languages, design and verification tools to enable non-cryptographic expert system architects and application developers to develop secure distributed applications leveraging advanced cryptographic techniques.

- Status: The Broad Area Announcement closes on December 1st.

Securely Taking on Executable Software of Uncertain Provenance (STONESOUP)

- How can we benefit from highly functional software produced by a globalized industry without putting the enterprise at risk?

STONESOUP Accomplishments

- Protects systems by automatically preventing software weaknesses from being exploited
- Automatically finds and mitigates exploitable security vulnerabilities in software
- Analyzes programs, not the data processed by programs
- Finds flaws that lead to insecure program conditions, rather than looking for known attack patterns
- Status: Program ended in 2015
- Tools are hosted online by NIST. Search IARPA STONESOUP NIST

Circuit Analysis Tools (CAT) and Rapid Analysis of Various Emerging Nanoelectronics (RAVEN)

- Microelectronics designs are advancing faster than our capacity to analyze them.

- How do we keep up with microelectronics when next generation circuits are 10,000x smaller than a human hair?

Circuit Analysis Tools (CAT)

- Develop tools for integrated circuit analysis at future technology nodes, specifically the 22 nm node and beyond.
  - Analysis tools capable of working with advanced packages including but stacked die.
  - Tools and techniques must address analysis and imaging challenges for which there are currently no solutions.
- Program Status
  - Program complete.
  - Commercial products are in the marketplace.

CAT
CIRCUIT ANALYSIS TOOLS

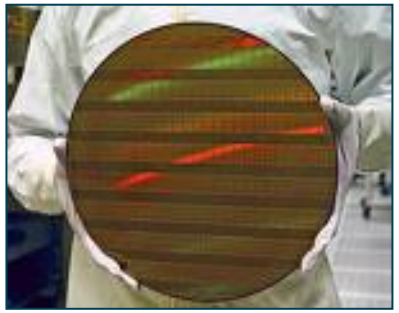
Rapid Analysis of Various Emerging Nanoelectronics (RAVEN)

- The RAVEN program aims to develop a prototype analysis tool for acquiring images from all layers in a 1 cm^2 area of a 14 nm integrated circuit, within 25 days.
- Program goals include: a fully automated prototype tool capable of rapid image acquisition from an individual chip.

Trusted Integrated Chips (TIC)

- Over 90% of the world's integrated circuit foundry capacity is controlled by non-US companies.

- How can we leverage this global infrastructure while protecting intellectual property and ensuring security?



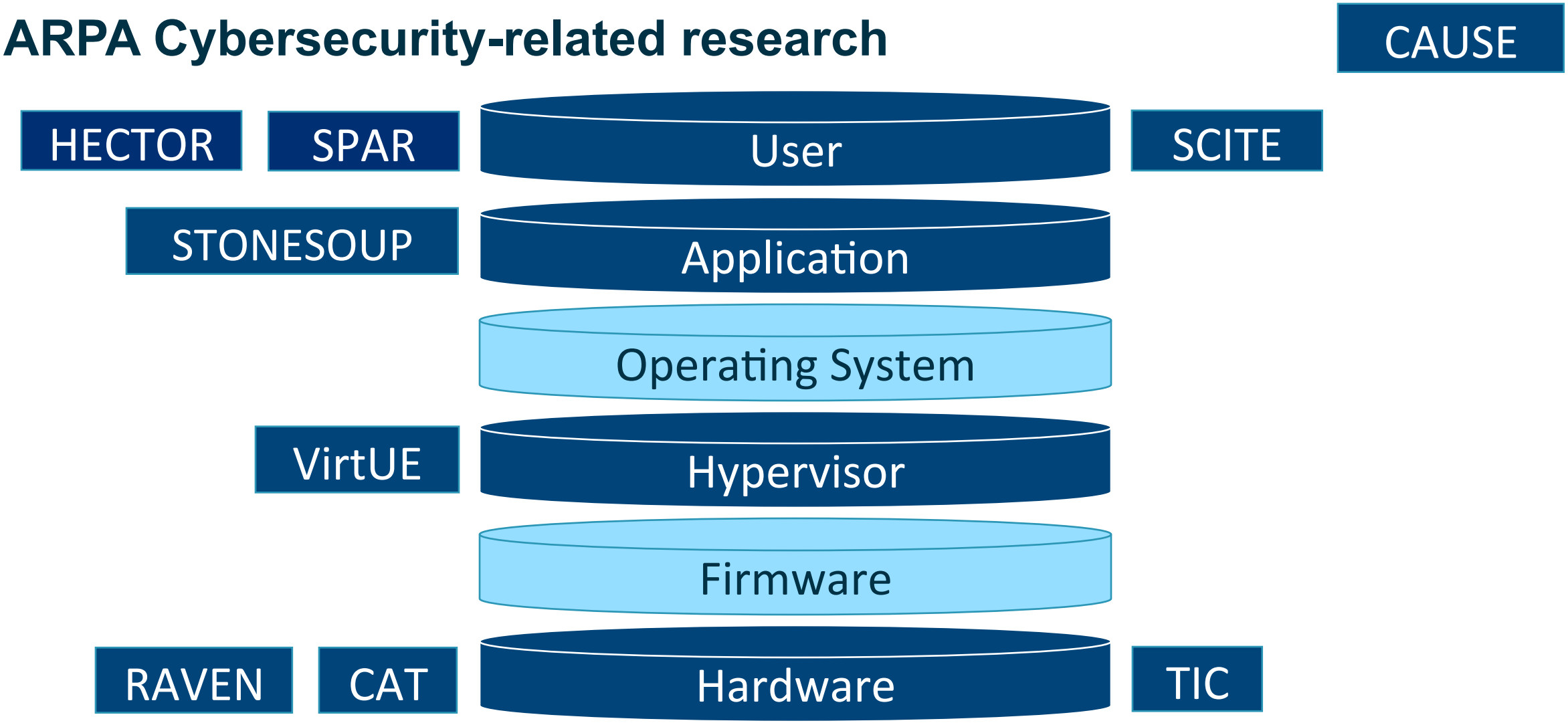
TIC Program Goals

- Ensure the U.S. Intelligence Community can obtain the highest performance possible in integrated circuits.
- Obtain assurance that designs are safe and secure – not compromised with malicious circuitry.
- Ensure security of designs, capability, and performance while simultaneously protecting intellectual property.
- Realize secure systems combining advanced CMOS with higher value chips.

TIC Technical Accomplishments

- Demonstrated split-manufacturing of integrated circuits using a state-of-the-art untrusted FEOL (Front End of Line) foundry and a trusted BEOL (Back End of Line) foundry.
  - 130 nm, 65 nm, and 28 nm nodes.
- Program Status
  - Program is in its final phase.
  - Findings are being shared with government and industry.

IARPA Cybersecurity-related research



How to Engage with IARPA

iarpa.gov | 301-851-7500

info@iarpa.gov

- Reach out to our Program Managers.
- Schedule a visit if you are in the DC area or invite us to visit you

Opportunities to Engage:

RFIS AND WORKSHOPS

Opportunities to learn what is coming, and to influence programs.

"SEEDLINGS"

Typically a 9-12 month study; you can submit your research proposal at any time. We strongly encourage informal discussion with a PM before proposal submission.

PRIZE CHALLENGES

No proposals required. Submit solutions to our problems – if your solutions are the best, you receive a cash prize and bragging rights.

RESEARCH PROGRAMS

Multi-year research funding opportunities on specific topics.