

# Hardware Support for Malware Defense and End-to-End Trust

## Cyber Security Division 2012 Principal Investigators' Meeting

October 11, 2012

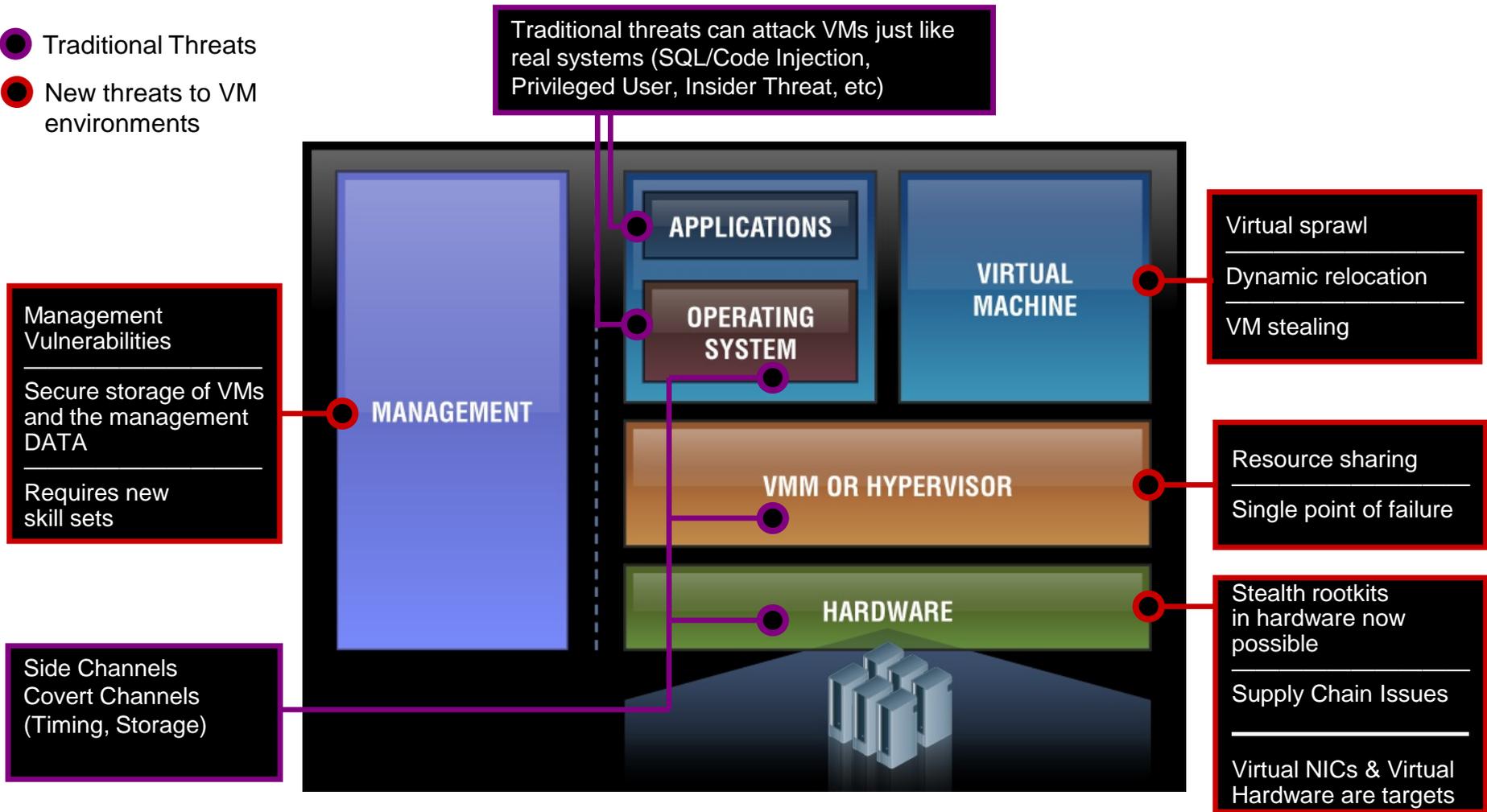
**Dimitrios Pendarakis**  
**Research Staff Member and Manager, Secure Systems Group**  
**IBM T.J. Watson Research Center**  
**dimitris@us.ibm.com**  
**914 784-7887**

# TTA 11 – Hardware-enabled Trust

- **Team make-up**
  - Dimitrios Pendarakis, PI
  - Rick Boivie
  - Kenneth Goldman
  - Eric Hall
  - Guerney Hunt
  - Mohit Kapur
  - David Safford
  
- **Group has a long history of research leadership and transition into products, standards and open source in areas:**
  - Operating systems, networking systems, NSFNET
  - Network security protocols, network scalability
  - Secure co-processors like the IBM 4758, 4764, ...
  - Trusted Computing and Linux Security
  - Secure Processors

# Virtualization & Cloud Vulnerabilities/Threats at the Platform Layer: Larger Attack Surface

- Traditional Threats
- New threats to VM environments

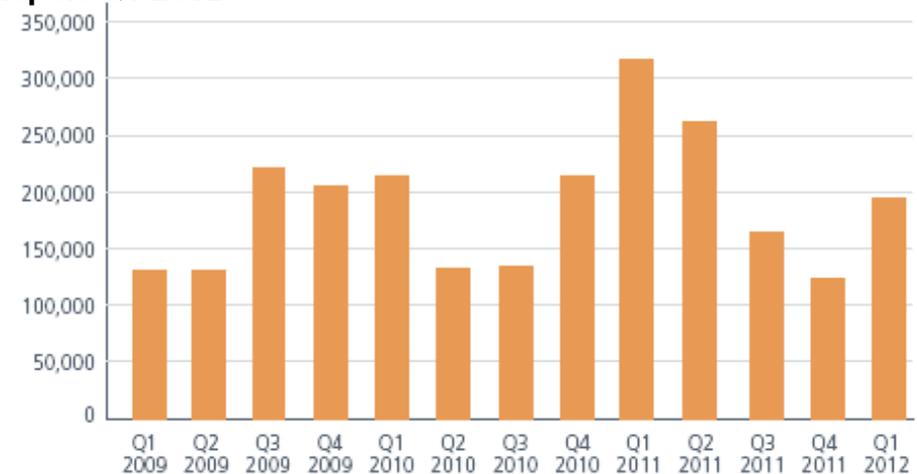
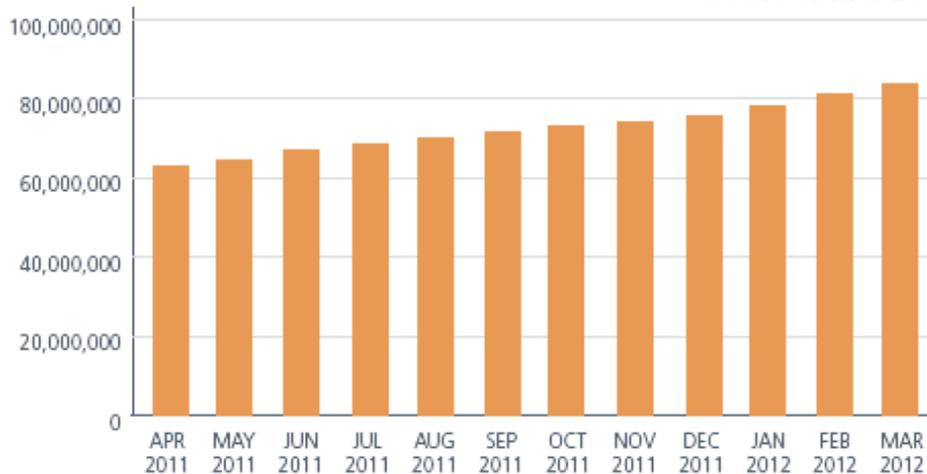


# Sample Threats: Rootkits, Sensors & Actuators

Total Malware Samples in the Database

Source: McAfee Report Q1 2012

Unique Rootkit Samples Discovered



~ 150,000 unique rootkits samples per quarter discovered

- Security threats in Sensor/Actuator systems: smart grid, oil & gas, transportation, water, medical devices, smart buildings, ...
  - Hacker Shows Off Lethal Attack By Controlling Wireless Medical Device
    - <http://go.bloomberg.com/tech-blog/2012-02-29-hacker-shows-off-lethal-attack-by-controlling-wireless-medical-device/>

Hackers Attack Servers of Oil Companies W  
2012-07-16

Hacker group Anonymous said it had successf  
servers of five oil and gas companies operating  
including Gazprom and Rosneft, posting hundr  
email addresses and passwords online.

Researcher releases smart meter hacking tool  
2012-07-20

Security consulting firm SecureState today releas  
source hacking tool that it claims will let security r  
penetration testers verify the security of electric uti  
meters being installed in millions of homes around

[http://www.us-cert.gov/control\\_systems/](http://www.us-cert.gov/control_systems/)

U.S. Critical Infrastructure Cyberattack Reports  
Jump Dramatically

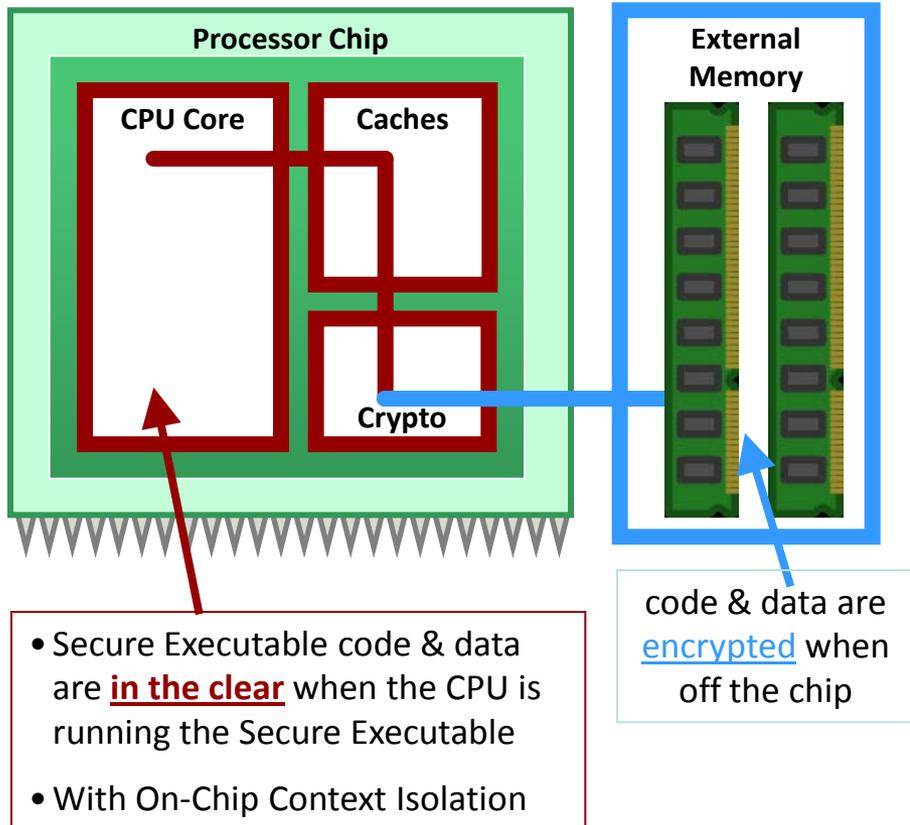
2012-06-29

U.S. critical infrastructure companies saw a dramatic increase in  
the number of reported cyber-security incidents between 2009 and  
2011, according to a new report from the U.S. Industrial Control  
System Cyber Emergency Response Team (ICS-CERT).

# Technical Approach: Problem

- **Common observations across all these vulnerabilities/threats/breaches**
  - Verifying the correctness of large software code bases is hard
  - Trusted Computing Base (TCB) is typically large: firmware, OS, hypervisor, etc.
  - Increasingly networked devices (e.g., control systems) present additional risks
- **Objective: Hardware Support for End-to-End Trust – from low end embedded devices to cloud servers**
  - **Trust:** Confidentiality and integrity of code and sensitive data
  - Introduce techniques to compartmentalize (isolate) sensitive applications
    - Minimize/reduce TCB
  - Perform continuous monitoring for anomaly detection; e2e measurement & attestation
- **Challenges**
  - Cost effective introduction of hardware changes; complexity of continuous monitoring
  - Architecture: integration of technologies to achieve trust properties from sensor to server
  - Enhancements in software stacks to take advantage of new capabilities

# Secure Blue++ w. On-Chip Context Isolation

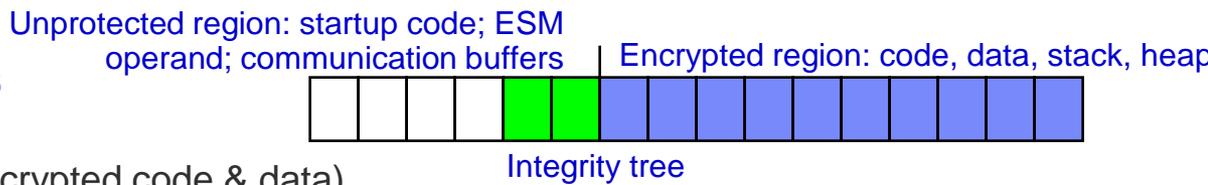


- Provides fine-grained crypto protection
- Protects confidentiality & integrity of an application's information so other S/W (including OS & malware with root privileges) can't read or tamper
- Minimizes Trusted Computing Base (TCB)
- Applications can use OS/Hypervisor services for I/O, scheduling, paging, interrupts etc.
  - Without trusting the OS with sensitive data
  - “Use but not trust” - analogous to the way we use the Internet via https
- Largely application transparent
  - New applications can be written or old app's re-built for stronger security;
  - Limit sensitive data leakage
- Limited H/W changes
- Low performance impact:
  - ~0 impact on cache hits, crypto latency impact on cache misses
    - **but only for 'secure applications'**
    - **0 impact for OS & 'regular apps'**

# Secure Blue++ & Secure Executables

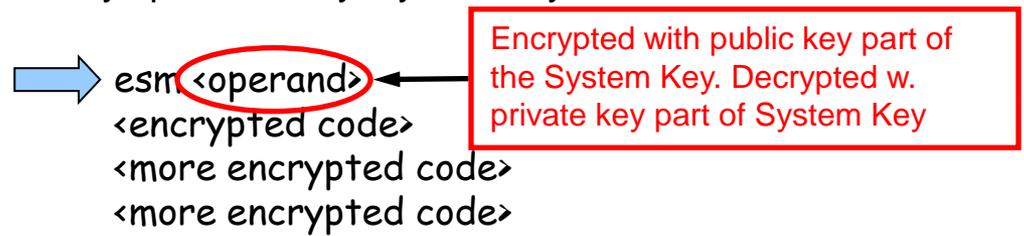
## Secure Executable Components

- Encrypted code & data
- Integrity tree (protects integrity of encrypted code & data)
- Some “startup code” that executes an ‘esm’ instruction

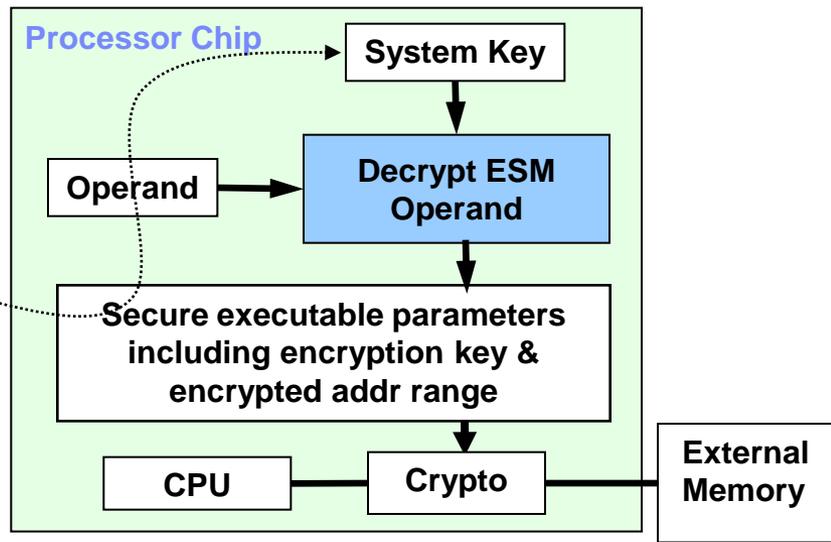


## Execution of ESM Instruction

- ESM Enters Secure Mode & loads crypto keys
- Keys are not “in the clear” in ESM instructions
- Keys protected by “system key” not available to S/W

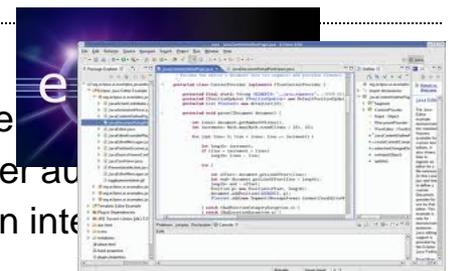


- Other S/W cannot decrypt the operand and get keys
- Other S/W cannot use the operand with other code

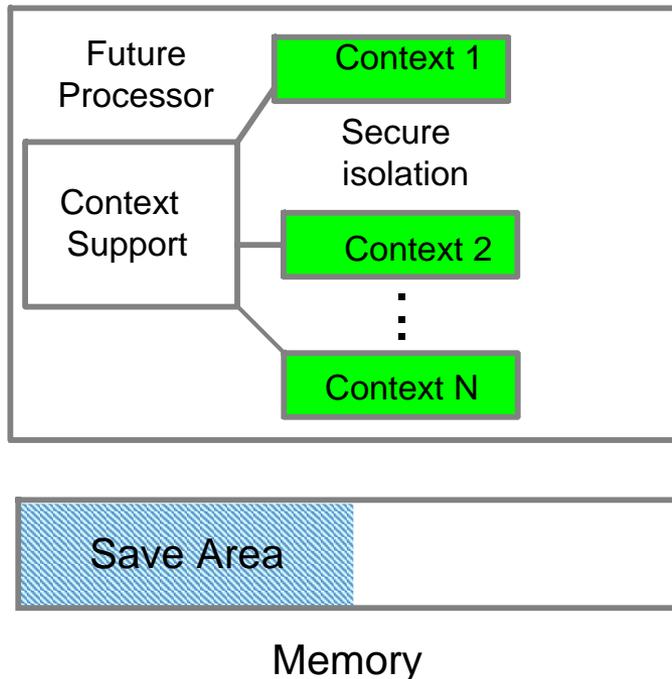


## SecureBlue++ Challenges

- Does not guarantee correctness of the “secure executable”; just protects it from ‘other’
- Does not protect against abuse of authenticated access; can be combined w. stronger au
- Adds some complexity to the S/W build / debug / mgmt and deployment lifecycle; can inte



# On-Chip Context Isolation

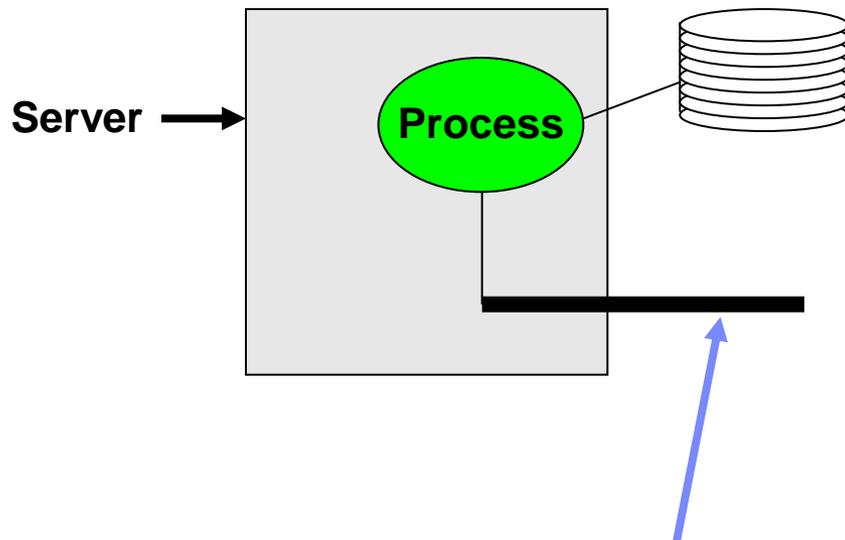


## Adds on-chip isolation to off-chip cryptographic isolation provided by SecureBlue++

- State in the CPU is tagged with a process ID.
- Each Process is assigned a unique save area
- A process never sees state from a different process without explicit permission.
  - Auto state save prevents access to another processes context.
- Cross context calls explicitly identify which registers are passed as parameters (both input and output).
- Contexts are reentrant
  - Specialized stack to enable interruptible context.
- Changes are “backward compatible” for existing kernels/OSes.

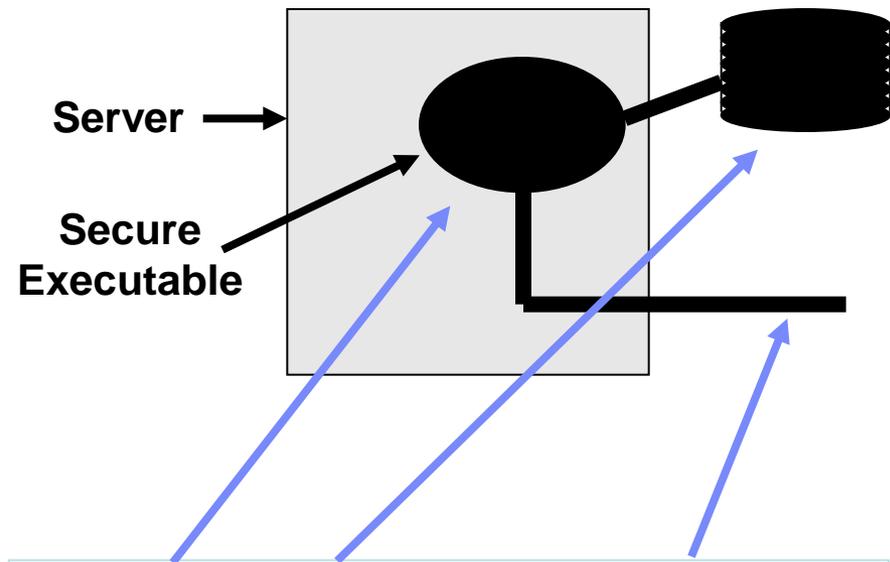
# End-to-end protection of sensitive information w. Secure Blue++ w. On-Chip Context Isolation

Today



Strong Crypto Isolation/Protection here

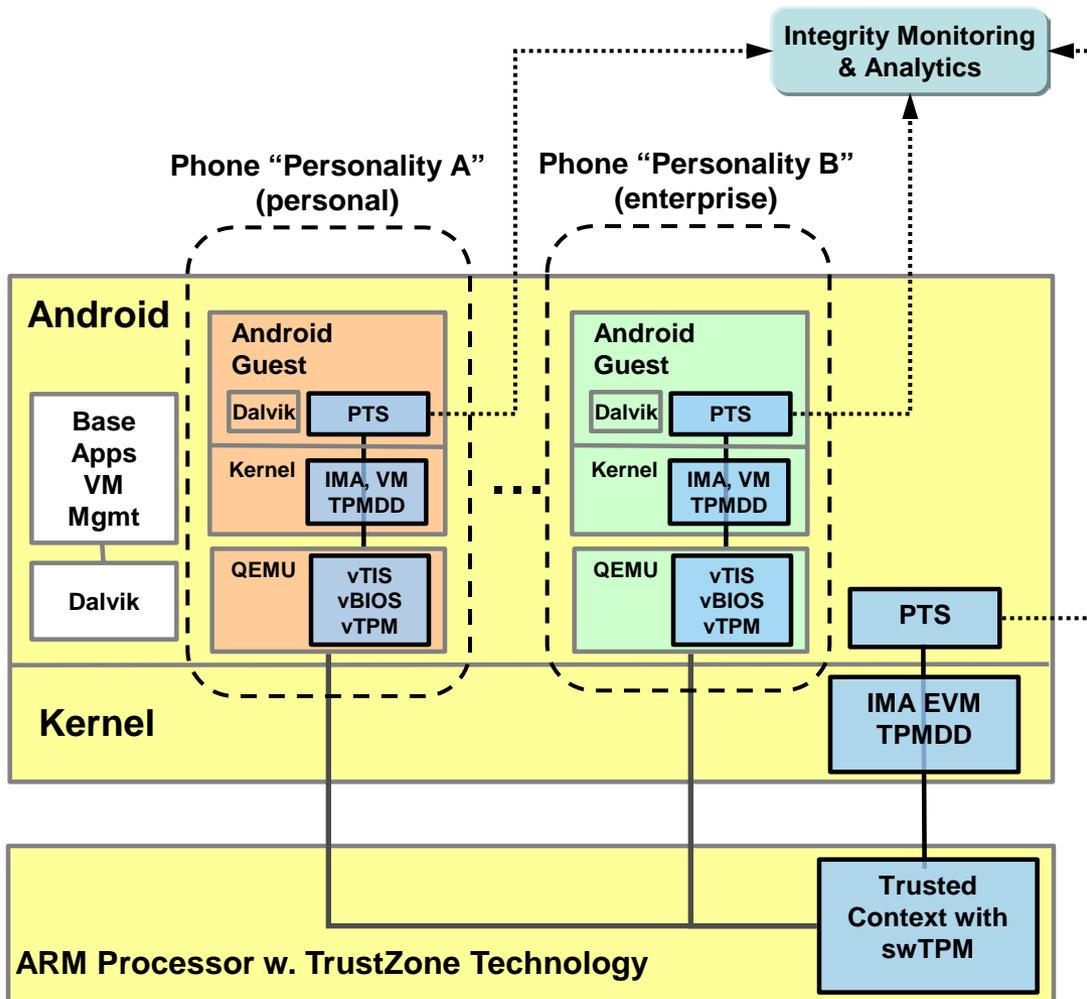
Secure Executables



Strong Crypto Isolation/Protection

- Keys & data always protected
- Private keys can't be stolen
- Certificates & public keys can't be tampered with

# Example Trusted Mobile Platform Architecture



## Trends

- Mobile platforms are full-fledged computers
- Bring-your-own-device (BYOD)
- Multi-personality devices (personal & corporate use)
- Simultaneous operation of potentially hostile applications
- Increase in mobile malware

## Approach

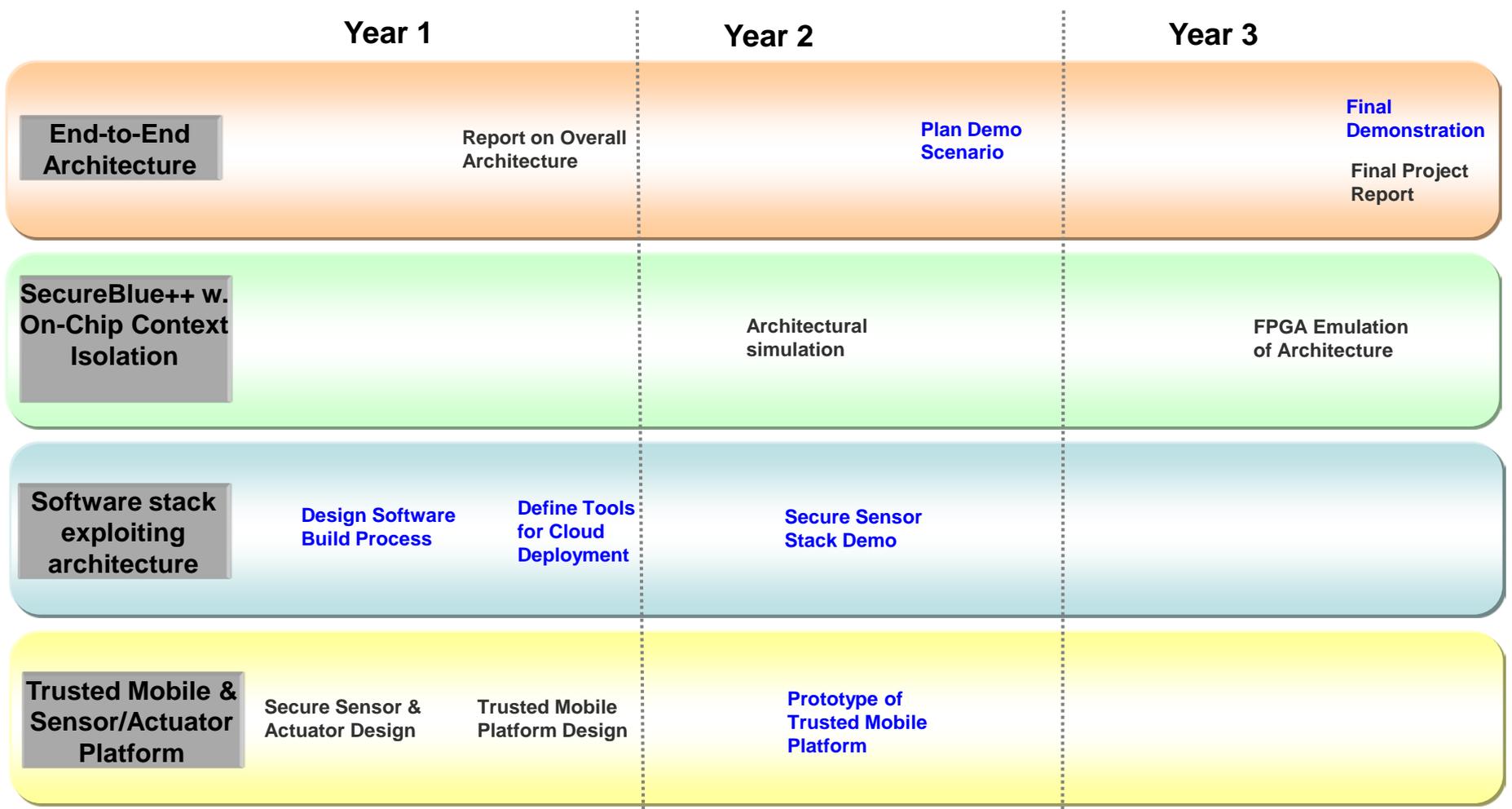
- Apply trusted virtualized architecture
- Provide similar trust properties as server platforms
- Isolate different "personalities"
- Continuous integrity monitoring and analysis

# “Trust Dust”



- Leverages a **hardware root of trust** for low-end sensors and actuators in a scalable, distributed management architecture
  - Continually tracks device state, identifies potentially compromised nodes & remediates violations
- Protects integrity of sensor and actuators in the “wild”; applicable to multiple IoT scenarios
- **Challenges:** cost effectiveness, scalability, integration w. security management tools

# Deliverables & Milestones



**Milestones**      **Deliverables**

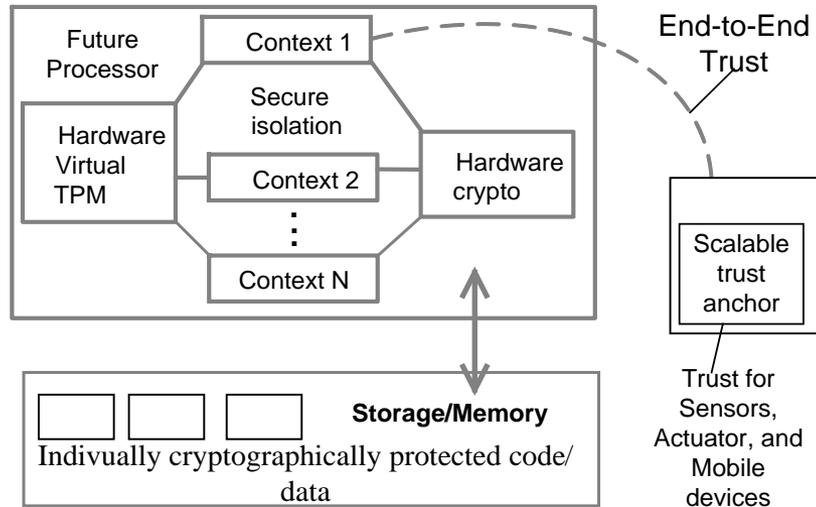
# Technology Transition Plan

- Investigate potential use of DETER testbed to evaluate the effectiveness of the architecture
- Publish proposed architecture
- Contributions to open source community
- Pursue commercialization within IBM
- Explore licensing or sale of selective technologies

# BAA Number: Cyber Security BAA 11-02 Offeror Name: IBM

## Title: Hardware Support for Malware Defense and End-to-End Trust

### Concept Graphic:



### Operational Capability

- Hardware Enabled Trust
  - Hardware to thwart attacks, untrusted cloud provider, and to protect sensors in the wild.
  - Hardware measure/attested context for end to end trust from cloud to sensors
- Low CPU performance Impact
- Minimal impact on cost
- Addresses TTA-11
  - End-to-end trust with hardware rooted measurements
  - *Enabling Hardware to thwart attacks with hardware isolated context with protection from HW and SW attacks*

### Proposed Technical Approach:

1. Create tamper resistant isolation with cryptographic confidentiality and integrity guarantees. Integrated hardware virtualized TPM provides end-to-end DRTM..
2. **Tasks:** Integrate and extend existing component technology simulations. Design/port hypervisor/linux for platform. Test resultant system for security and performance.
3. **Status:** Components exist at different levels (shipping, prototyped, simulated, designed).
4. IBM has already designed and simulated several isolation mechanisms, and demonstrated trusted sensors.
5. IBM has been leading the Linux implementation of Trusted Computing, and integrating the necessary hardware in products.

### Schedule, Cost, Deliverables, & Contact Info:

Period of performance, Milestones and total costs:

Total Period 3 years

Milestones:

- Year 1: Design and prototype system architecture by merging component technologies
- Year 2: SW Modifications for new hardware
- Year 3: test security and performance of system

Deliverables: Prototype trusted endpoint, simulation of end to end architecture, test results using system and application software

Corporate Information: IBM

POC Dimitrios Pendarakis, Yorktown Heights, NY, 10532, phone (914) 784-7887, email dimitris@us.ibm.com