

Hardware Enabled Zero Day Protection



Cyber Security Division 2012 Principal Investigators' Meeting

October 11, 2012

Paul A. Rivera
President/CEO
Def-Logix, Inc.
Email: privera@def-logix.com
Phone: 210-478-1369

Introduction

- Company founded in 2008
- Based out of San Antonio, Texas
- Primary customer is USAF



Team

Team Member	Roles	Background
Paul Rivera (KEY)	Program / Project Manager and Principal Investigator	16+ years of Computer and network security research and development. Specializing in development and testing of Intrusion Detection/Prevention Systems, Network Vulnerability scanners and Network Analysis tools.
Jeffrey Samas (KEY)	Principal Engineer Project Lead of First Responder and Entrap components.	20+ years as an accomplished software developer. Extensive experience in the full SDLC, coding standards, software configuration management, and project management in the cyber security domain, and has specific experience building kernel level applications and Host Based Security System (HBSS) integration.
Kevin Borden	Director/Principal Engineer Project Lead of Enterprise Integration (HBSS integration)	20+ years of experience in software engineering. Lead developer of DISA's Asset Configuration Compliance Module (ACCM). Extensive development experience with McAfee SDK and HBSS module development.

Team

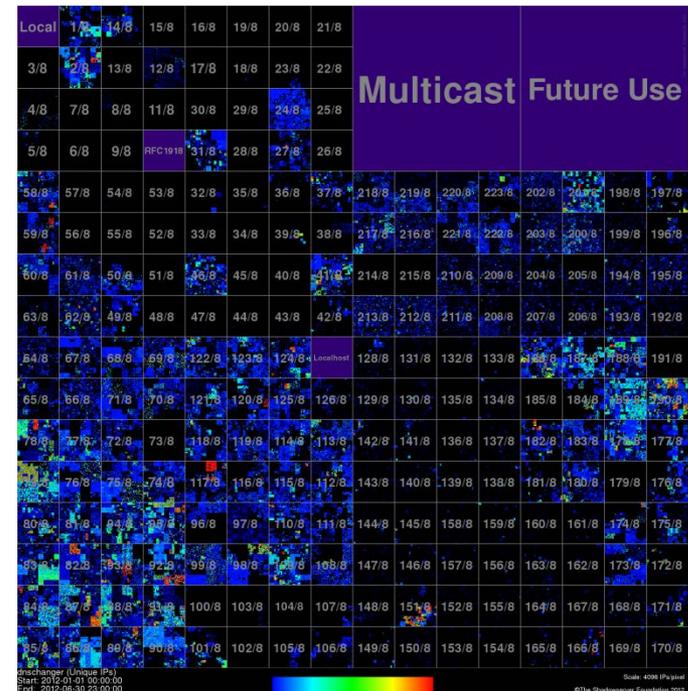
Team Member	Roles	Background
Nicholas Navarro (KEY)	Software Engineer Project Lead of Shimmer and Phoenix Components	13+ years of experience in information security. Specializing in developing both network security applications and infrastructure solutions. Experienced developing MS Windows kernel/driver level and UEFI applications.
Adrienne Young	Software Engineer Developer on Shimmer and Phoenix components	16+ years as a software engineer specializing in Cyber security. Designed applications for real time monitoring and device control. Experienced developing digital forensic and UEFI applications.
David Clark	Testing Engineer Project Lead of Quality Assurance	4+ years of unit testing, integration testing, functional testing, system testing, acceptance testing and automated regression testing.
Thomas Rognon	Software Developer User Interface Development	9+ years of experience developing user interfaces and automation.
Paul Graves	Technical Writer	5+ years of experience developing, gathering, and disseminating technical information among customers and software engineers. Specializing in developing training material, configuration requirement specifications, user and installation guides.

Technical Topic Area

- TTA #11 Hardware Enabled Trust
- Hardware can be the final sanctuary and foundation of trust in the computing environment.
- Hardware can provide a game changing foundation to build on future cyber infrastructure
- Current technology under utilize hardware capabilities to provide trust and system security.
- Hardware security solutions will be harder to break and increase the difficulty for an attacker to compromise systems.
 - End-to End Trust
 - Enabling hardware to thwart attacks
 - Hardware enabled Resilience

Malware is Evolving

- MS Windows is forcing malware authors to develop new sophisticated new tactics, reaching deep into OS internals.
- Bootkits like TDL4 arose from the need to circumvent Windows Patch Guard. DNS Changer infection showed the power of this technique.
- Worse is to come: BIOS malware will likely arise in response to Windows 8 secure boot.
- Proof of concept BIOS malware “Rakshasa” (Blackhat 2012) has the ability to infect multiple firmware, giving it the ability to survive HD format and BIOS flashing.



IPV4 DNS Changer Infection Map

Solution

Host Layers

Def-Logix Technologies

Ring

User Space

OS libraries and executables

First Responder

responds to compromise and interfaces with enterprise security architecture

Kernel Space

system and device drivers

Entrap

prevents malicious code from executing

UEFI Application

Firmware, BIOS and VMM

Shimmer

detects compromise and restores the system

UEFI Drivers

NIC, SATA and graphic cards

Phoenix

protects Shimmer

3

0

-1

-2

OS

UEFI

Hardware

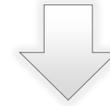
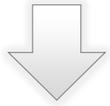
Full Spectrum Protection

First Responder

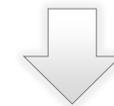
Process Injection

Keyboard Logger

Benign Call



API/Windows RT Monitoring



Windows Kernel

Entrap

Applications

Application
Hybrid
Sandbox

Pass-to-Hash

Anti-Virus

Security
Programs

Kernel
Structures

IDT
Interrupt
Descriptor Table

SSDT
System Service
Dispatch Table

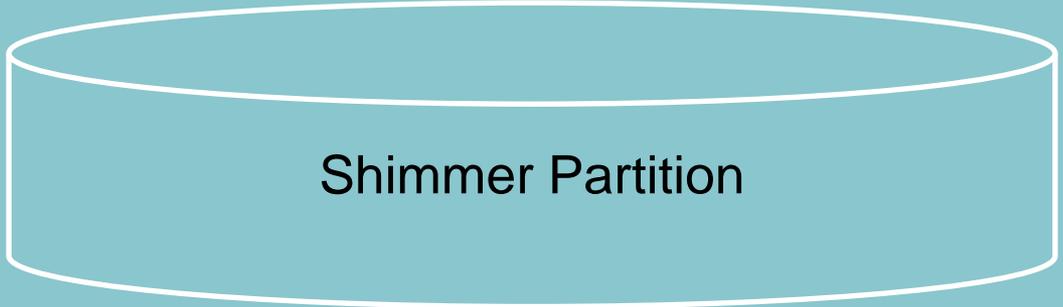
IRP
I/O Request
Packets

**Shadow
SSDT**

Shimmer

Shimmer
Application

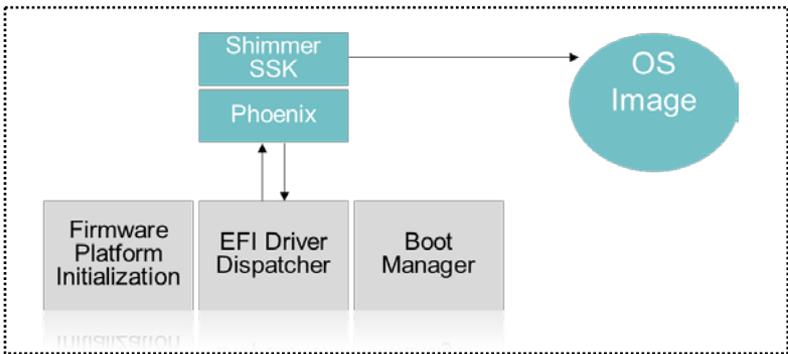
Security Kernel



Shimmer Partition

The diagram shows a 3D cylinder representing a partition. The cylinder is outlined in white and is centered in the lower half of the slide. The text 'Shimmer Partition' is written in black inside the cylinder.

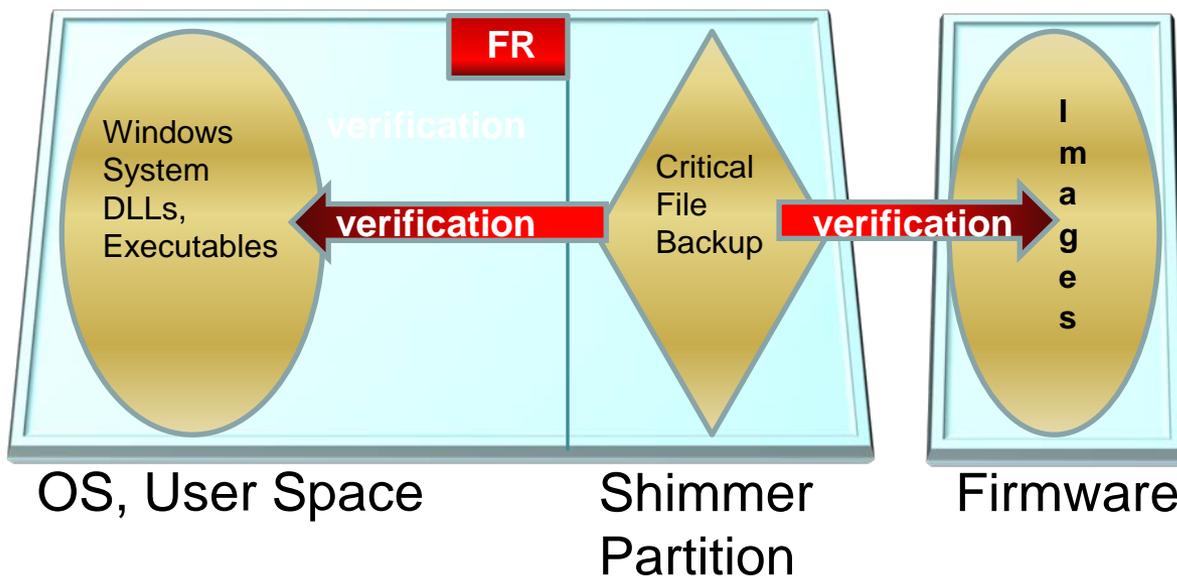
Shimmer Con't



Network



Hard Drive



UEFI Communication

McAfee ePO



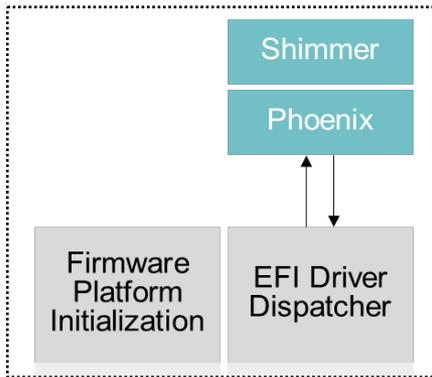
First Responder

Windows UEFI Aware

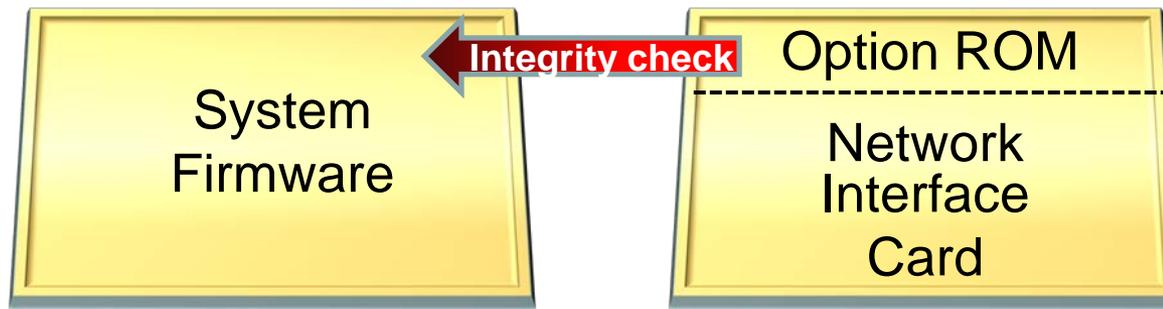


UEFI Applications/Hardware

Phoenix

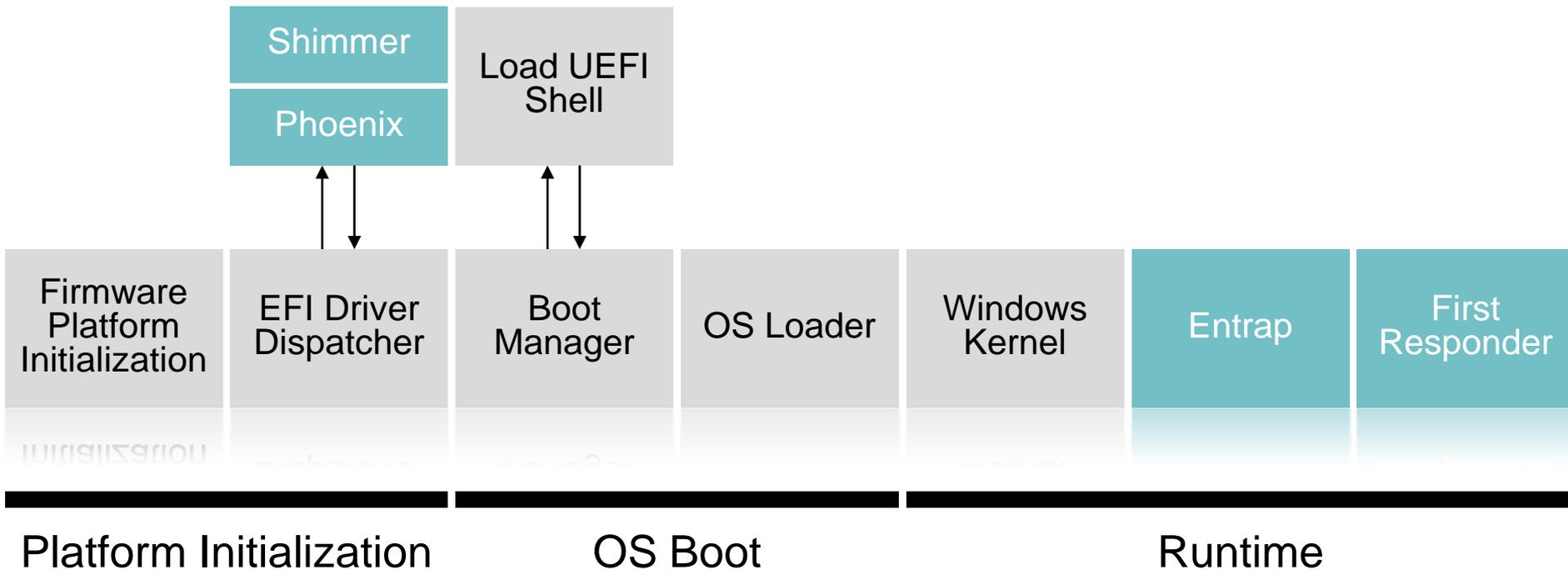


Off-CPU Validation

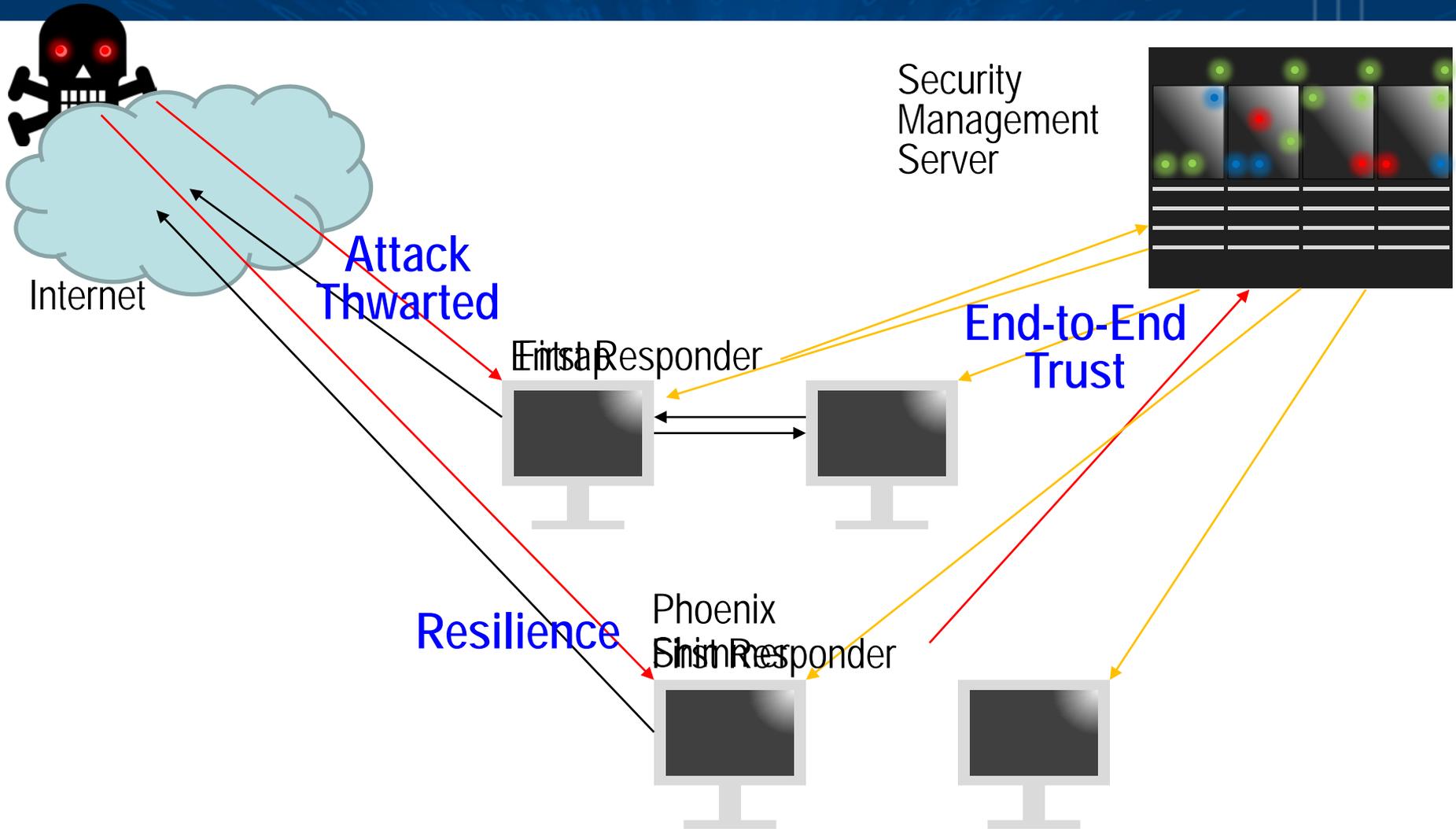


Prior to OS Control

HEZDP in action



HEZDP in the Enterprise



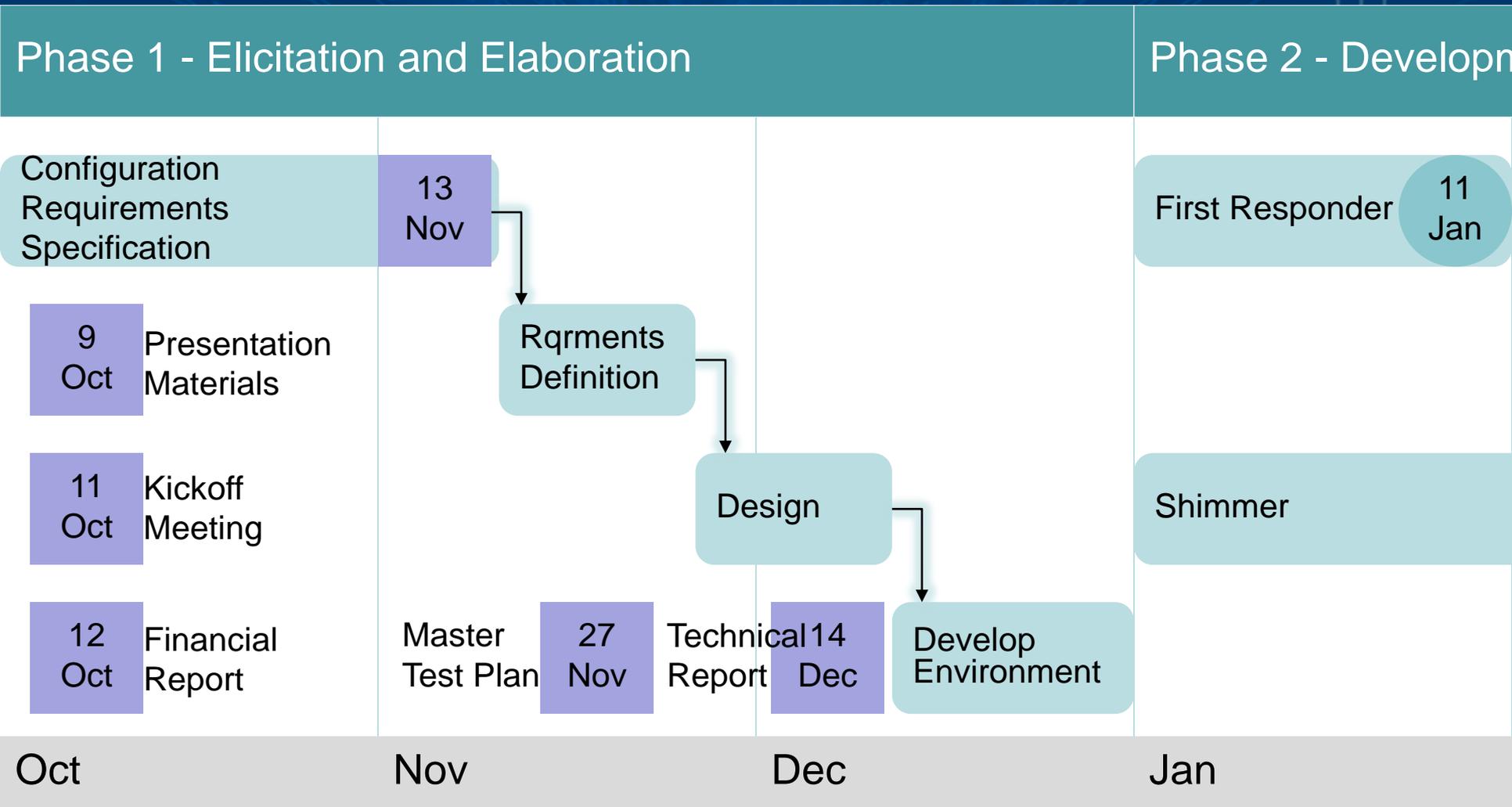
TTA Criteria

BAA-TTA-11 Question	First Responder	Entrap	Shimmer	Phoenix
Is the system secure?				
Is it in good standing?				
Is it trustworthy? Even if "broken" in the future, can past operations be trusted?				
Is the system genuine?				
What was its path from manufacturing to system prototype demonstration in an operational environment?	N/A	N/A	N/A	N/A
Was the design of its elements compliant with the best industry and technology practices?				

Technical Challenges

- Legacy BIOS and Option ROM device support.
 - The Compatibility Support Module (CSM) is provided to address the two key technical issues.
- Instability and Recovery
 - Shimmer recovery toolset
- Existing Infrastructures and Legacy OS support
- Securing the UEFI Partition
 - Disable 'mountvol' command. Control access to UEFI partition
 - Encryption
 - Firmware password
- Enterprise Level Deployment

Schedule



Milestones

Milestone	Date	Comment
Prototypes		
• First Responder	11 Jan 2013	
• Entrap	11 Feb 2013	
• Shimmer	11 Mar 2013	
• Phoenix	11 Apr 2013	
HBSS Integration	1 May 2013	Infrastructure Support
ePO Integration	4 Jun 2013	GUI, Deployment, Console Management
Fieldable Prototype	2 Jul 2013	Begin Final Field Regression Testing

Deliverables

Item	Deliverable	Date	Comment
A001	Financial Report	12 Oct 2012	Initial Report, followed by Monthlies
	Technical Report	14 Dec 2012	Initial Report, followed by Quarterlies
A002	Presentation Materials	9 Oct 2012	
A003	CRS	13 Nov 2012	Configuration Requirements Specification
A004	Master Test Plan	27 Nov 2012	
A005	User Guide	12 Apr 2013	
	Installation Guide	12 Apr 2013	
	Release Notes	12 Apr 2013	
A006	Initial Release	11 Oct 2013	Binaries, Source, Packaging Information
A007	Final Release	11 Feb 2014	

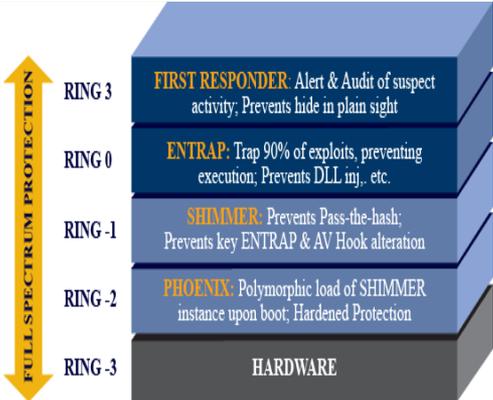
Deliverables

Deliverable	Date	Comment
Kickoff Meeting	11OCT12	
Status Review Meetings	Quarterly	Dates to be set by AFRL PM
Interim Meetings	TBD	Schedule/Medium to be set by AFRL PM
Interim Deliverables	Quarterly	Dates to be set by AFRL PM

Technology Transition

- DETER Lab
- PREDICT and SWAMP
- Government
 - Pilot in DISA, DoD and/or USAF
- Colleges and Universities
 - Build relationships with local universities and colleges
- Commercial
 - Leverage existing relationship with McAfee Software Innovation Alliance (SIA)

Quad Chart

<p>BAA Number: Cyber Security BAA 11-02 Title: Hardware Enabled Zero-Day Protection (HEZDP)</p>	<p>Offeror Name: Def-Logix, Inc Date: July 7, 2011</p>
 <p>Each layer ensures integrity of the layer above <small>(Blue: lab operational; Light Blue: initial R&D)</small></p>	<p>Operational Capability:</p> <ol style="list-style-type: none"> Performance targets: Prevention of exploits, defense against pass-the-hash and AV Bypass techniques. Quantify performance for key parameters: Prevent 90% of exploits. Stop lateral movement via Pass The Hash (PTH). Secure integrity of AV and other host based defense systems. Cost of ownership: Leverages existing deployed technology reducing overall costs. HEZDP technology adheres to multi-tiered license model to maximize adoption across organizations. Addresses BAA goals: Fulfills TTA 11 goals providing a holistic approach in combating malicious activity.
<p>Proposed Technical Approach:</p> <ol style="list-style-type: none"> Provides layered defense from Ring -2 to Ring 3. Protects against exploits. Protect against Pass-the-Hash and AV Bypass Techniques. Existing commercial solutions are easily bypassed as they lack appropriate Ring -1 and Ring -2 defenses. Extend Entrap to prevent of exploits. Develop Shimmer to ensure integrity of Entrap and AV structures as well as provide protection against Pass-the-Hash. Develop Phoenix to provide out-of-band integrity checks. Integrate into enterprise management frameworks such as McAfee ePO. Protects against 70% of exploits Entrap near completion. First Responder, Phoenix and Shimmer are in initial R&D stages & 5. Internal R&D. 	<p>Schedule, Cost, Deliverables, & Contact Info:</p> <p>Type II Proposal. 21 month effort, first operational prototype after nine months. v1.0 deliverable 18 months after award. v1.1 delivered upon completion.</p> <p>Deliverables: Includes software binaries and executable; Complete user and administrative documentation, Final Technical Report.</p> <p>Corporate Information: Def-Logix, Inc. 10010 San Pedro, Suite 510 San Antonio, TX 78216 Technical POC: Paul A. Rivera Technical POC email: privera@def-logix.com Technical POC Phone: 210-478-1369</p>

Questions

