

Generic IP independent BIOS Signing and Parsing

Gahan Saraiya

Institute of Technology
Nirma University

May 10, 2020

Outline

1. About the Project
2. Motivation
3. BIOS: Basics
4. Requirement Specification
5. My Contribution
 - Setup Knobs Modification
 - Implementation of Parsing
 - Runtime UEFI Variable Creation
6. Future Scope



About the Project

In general to generate BIOS image (*.rom file), compilation of XYZ.c (source code) has to be done, this compilation not only involves compilation of DXE driver, PEI driver, EFI Application but also includes pre-processing checks, compression of raw files which takes huge amount of time depending on the system configuration. Implementation of this project aids in reduction of this compilation time.



- ▶ BIOS development Team
- ▶ Automation Team
- ▶ Validation Team
- ▶ Other Development Team



Motivation: Issues/Challenges to the industry (Towards my contribution)

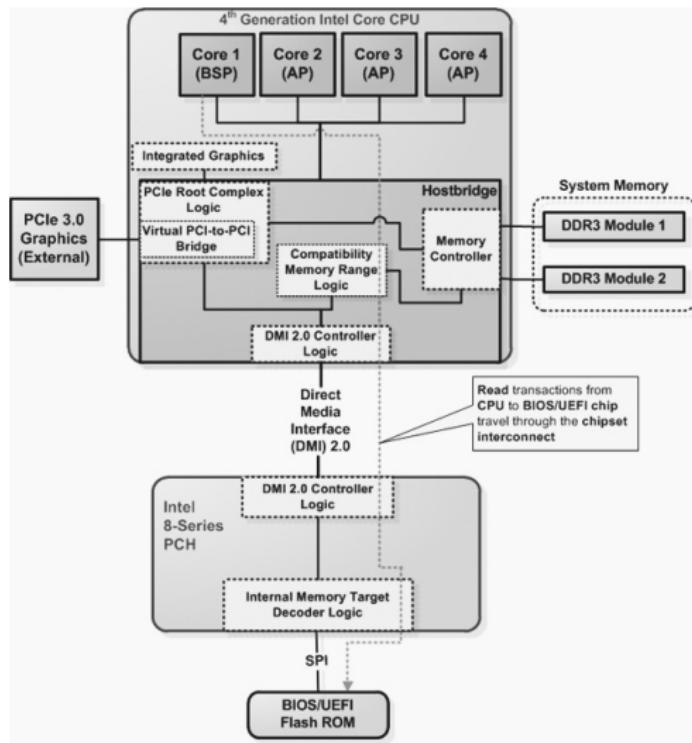
- ▶ BIOS image generation: Compilation of whole source code
- ▶ More Time complexity: Compilation of source code to generate BIOS image
- ▶ Accessing and modifying BIOS Setup Option(s) remotely
- ▶ Firmware Flashing of BIOS remotely
- ▶ Updating CPU microcode
- ▶ Summarizing changes among BIOS image
- ▶ Avoiding exposing the source code support
- ▶ Avoid setting of BIOS development platform for stake holders
- ▶ Runtime BIOS Support for temporary UEFI variable creation



- ▶ Set of Software Routines
 - ▶ Initialize and test hardware on start
 - ▶ Provides the OS with a generic hardware abstraction
- ▶ the BIOS must do its job before your computer can load its operating system and applications

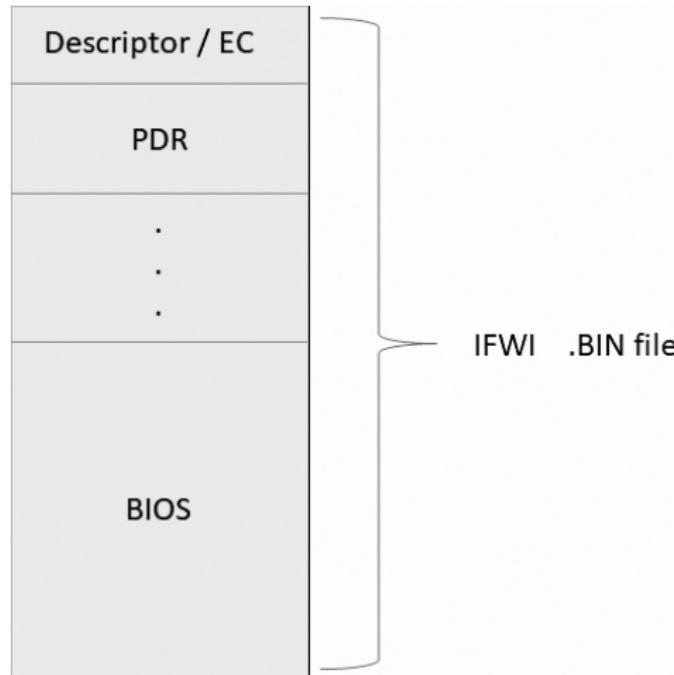


BIOS: Architecture



3. BIOS: Basics

BIOS: Firmware Image



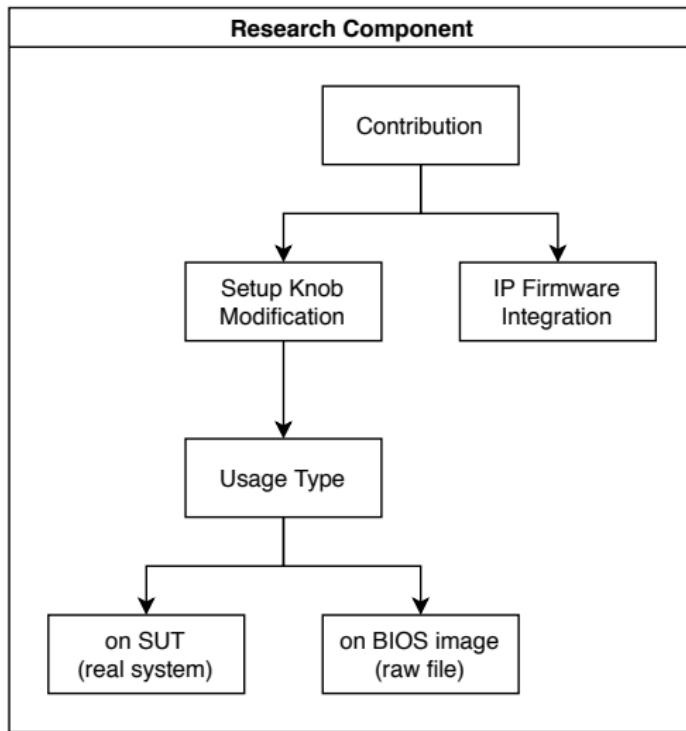
Requirement Specification

- ▶ Visual Studio C/C++ IDE
- ▶ Visual Studio Code
- ▶ Python 3
- ▶ Memory Access Interfaces¹

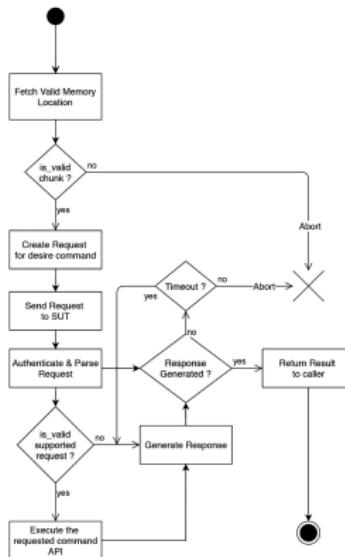


¹itp, itp2, windows, linux, ltb, dci, efi shell, etc.

My Contribution towards issues/challenges



Setup Knobs Modification: Process Flow I



Setup Knobs Modification Flow on SUT

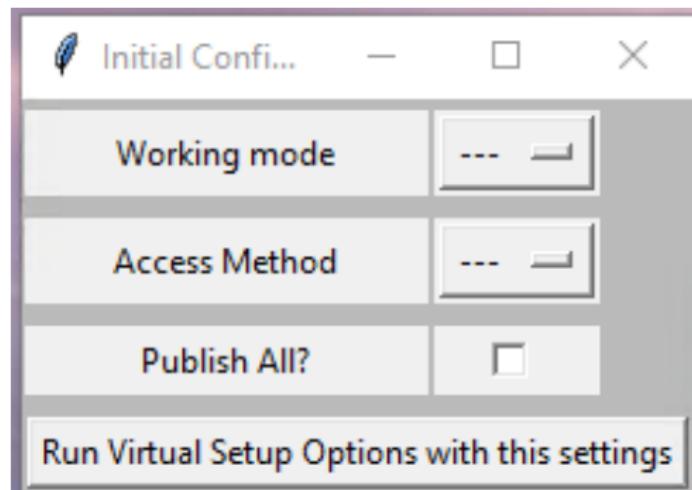


Implementation of Parsing: Additional Tech Stack

- ▶ Tkinter
- ▶ XML
- ▶ Decompression binaries



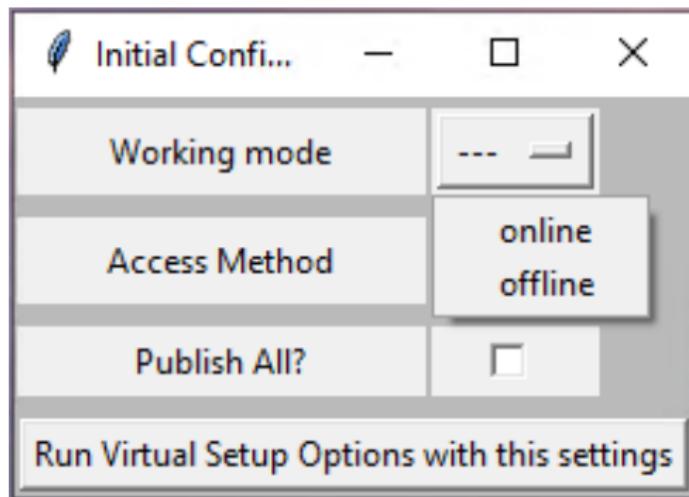
Setup Knobs Modification: Implementation Snaps I



Menu to Select initial configuration for work



Setup Knobs Modification: Implementation Snaps II



Available work mode for the system: Online and Offline



Setup Knobs Modification: Overview of GUI Actions

Button	Interpretation
Push Changes	Apply changes to system if online mode else apply changes to 'bin' file
View Changes	View saved changes in new window
Exit	Exit the GUI
Reload	Reload the GUI
Discard Changes	Discard any change made, any value if modified are restored to current value
Load Defaults	Restore to default values and revert any changes made

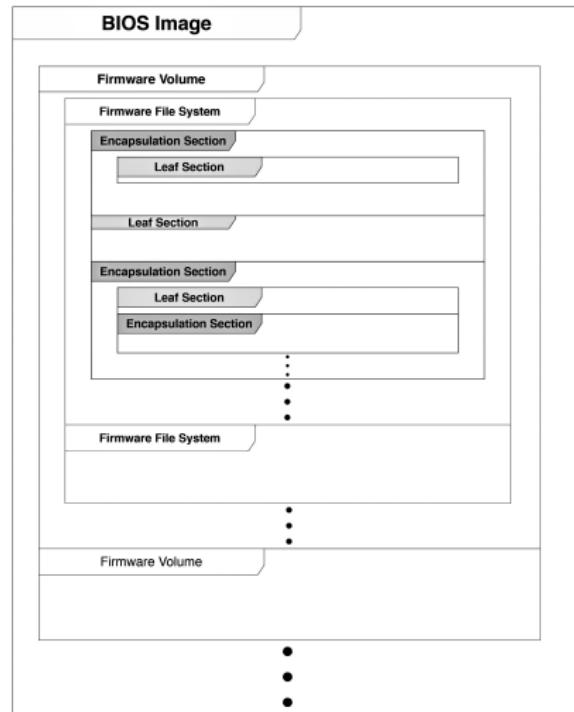


Setup Knobs Modification: Outcome

- ▶ Cross platform usage
- ▶ API as a driver in BIOS Firmware
- ▶ Generic solution for usage types - on **SUT**, on **BIOS image**
- ▶ Information parsing and simulation
- ▶ Realtime sync for simulation changes
- ▶ Seamless Integration



Implementation of Parsing: Format of BIOS Image

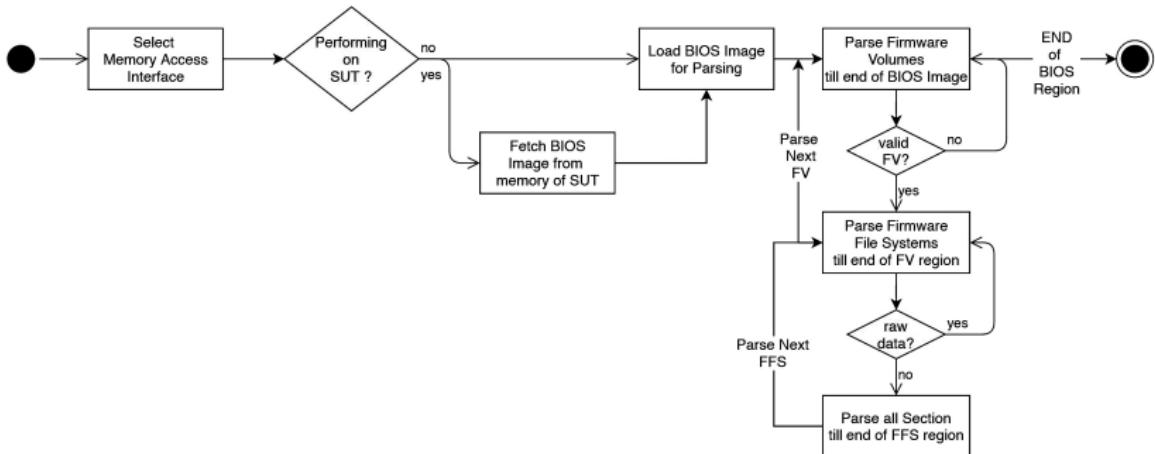


5. My Contribution

b) Implementation of Parsing



Implementation of Parsing: Work Flow

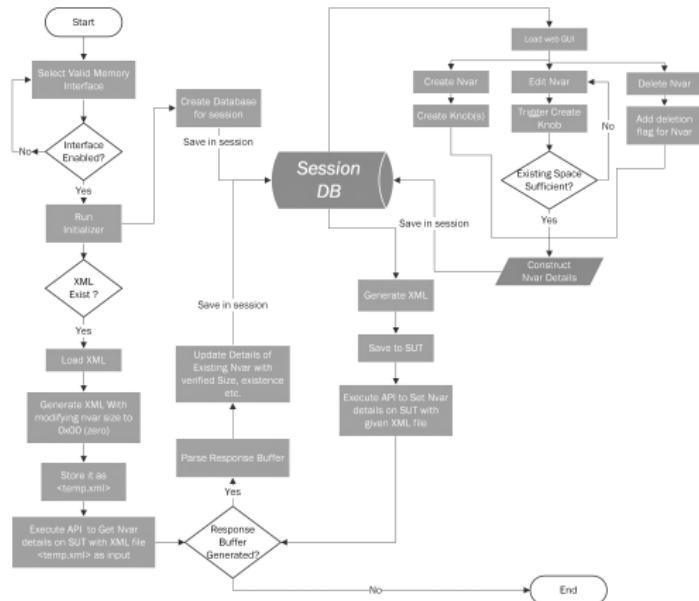


Outcome

- ▶ Human Readable interpretation of BIOS Image
- ▶ GUIDs Lookup
- ▶ Verification of existence of module by GUID
- ▶ Storing the image file system content by GUID
- ▶ Summarizing changes of two BIOS image



Runtime UEFI Variable Creation: Work Flow



Gahan Saraiya

5. My Contribution

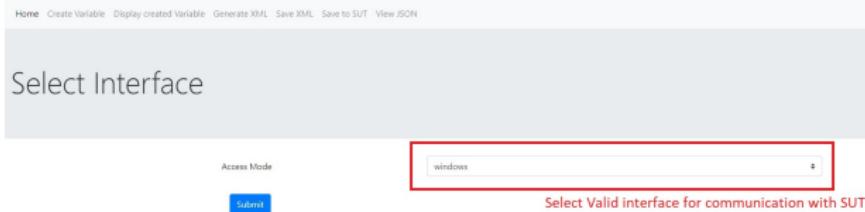
c) Runtime UEFI Variable Creation

Runtime UEFI Variable Creation: Additional Tech Stack

- ▶ Flask
- ▶ Ajax
- ▶ jQuery
- ▶ Javascript
- ▶ HTML/CSS
- ▶ XML
- ▶ JSON



Runtime UEFI Variable Creation: Implementation Snaps I



Home Page to Create UEFI Variable



Runtime UEFI Variable Creation: Implementation Snaps II

Home Create Variable Display created Variable Generate XML Save XML Save to SUT View JSON

User Created Options

Currently displaying only Variable which are existing on SUT. To view all the Variables [click here](#)

Interface selected successfully

Unique Id	Name	GUID	Size	Knob Details
demo_0x0003f07e-0x82f7-0x11ea-0x8e-0x6c-0x00-0x0a-0xcd-0x33-0x38-0x26	demo	0x0003f07e-0x82f7-0x11ea-0x8e-0x6c-0x00-0x0a-0xcd-0x33-0x38-0x26	2 (0x2)	View Delete
			11 (0xb)	View Delete

Variables created or exists on SUT

5. My Contribution

c) Runtime UEFI Variable Creation

Runtime UEFI Variable Creation: Implementation Snaps III

[Home](#) [Create Variable](#) [Display created Variable](#) [Generate XML](#) [Save XML](#) [Save to SUT](#) [View JSON](#)

Create Variable

Variable name	<input type="text" value="Enter Variable Name (only alphabets and numbers allowed)"/>
GUID	<input type="text" value="0xbff24c0b-0x873c-0x11ea-0x90-0x8e-0x00-0x0a-0xcd-0x33-0x38-0x26"/>
Attributes	<input type="text" value="0x7"/>
<input type="button" value="Submit"/>	

Create new UEFI Variable on SUT



Gahan Saraiya

5. My Contribution
c) Runtime UEFI Variable Creation

18MCEC10

23/32

Runtime UEFI Variable Creation: Implementation Snaps IV

The screenshot shows a user interface for managing UEFI variables. At the top, a navigation bar includes 'Home', 'Create Variable', and 'Display created Variable'. The main area is titled 'User Created' and displays a table of variables. A modal window titled 'Details' is open, showing the configuration for a variable named 'oneVar'. The 'Details' table has columns for Unique Id, Name, Type, Offset, Size, Default Value, Current Value, Description, and Edit/Delete buttons. The 'oneVar' row is highlighted with a red border. Below the table, a message says 'Options(s) Created under the created Variable'. The 'Edit' button for the 'oneVar' row is also highlighted with a red box. The background shows a list of variables with their unique IDs and sizes, and a 'View' button for each, which is also highlighted with a red box. A message at the bottom of the interface says 'Interface selected successfully'.

Unique Id	Name	Type	Offset	Size	Default Value	Current Value	Description	Edit	Delete
oneVar	oneVar	checkbox	0 (0x0)	1 (0x1)	0 (0x0)	0 (0x0)	descript	Edit	Delete
ReservedSpace	ReservedSpace	reserved	1 (0x1)	10 (0xa)	1 (0x1)	1 (0x1)	Reserved Space within the Nvar	Edit	Delete

Options(s) Created under the created Variable

Interface selected successfully

Unique Id	Name	Size	Knob Details
demo_0x0003f07e-0xb2f7-0x11ea-0x8e-0x6c-0x00-0x0a-0xcd-0x33-0x38-0x26	demo	0x0003f07e-0xb2f7-0x11ea-0x8e-0x6c-0x00-0x0a-0xcd-0x33-0x38-0x26	11 (0xb) View Delete

Options listed under Variable

Runtime UEFI Variable Creation: Implementation Snaps V

Variable name	demo	Type	Offset	Size	Default Value	Current Value	Description	Edit	Delete		
Guid	0x0003f07e-0x02f7-0x11ea-0x8a-0x5c-0x00-0x0a-0x33-0x38-0x26	oneVar	oneVar	checkbox	0 (0x0)	1 (0x1)	0 (0x0)	0 (0x0)	descript	<button>Edit</button>	<button>Delete</button>
Size	11 (0xb)										
Is_exist	True (0x1)										
Attributes	7 (0x7)										
Name	oneVar										
Value	checkbox										
Current_value	0 (0x0)				<button>Change</button>	<button>Save</button>	clicking this button will enable the input to change current value Changed value will be saved when Clicked on save button				
Size	1 (0x1)										
Offset	0 (0x0)										
Description	descript										

Edit the Existing Option Created under Variable SUT

Runtime UEFI Variable Creation: Implementation Snaps VI

Create Option

Select Detailed options

Option(s): 2, two Add Option

Value: 1 - one, 1 - one (selected), 2 - two

Done Discard

Variable name: anotherVar

Guid: 0x... (0x9405d39-0x8740-0x11ea-0xb8-0x...)

Attributes: 7 (0x7)

IsExist: False

Size(0x0): 0 (0x0)

Option Type: oneof oneof

Name: Enter Name of the...

Description: Enter Description for the...

Size(0x1): 1

Offset(0x0): 0

Submit Save and Create

Create New Option(s) under Variable - Oneof Type

Runtime UEFI Variable Creation: Implementation Snaps VII

Create Option

Variable name: anotherVar

Guid: 0xa0455d9-0x5740-0x11ea-0xb8-0x

Attributes: 7 (0x7)

IsExist: False

Size(0x0): 0 (0x0)

Option Type: numeric

Name: Enter Name of the [REDACTED]

Description: Enter Description for the [REDACTED]

Size(0x1): 1

Offset(0x0): 0

Submit Save and Create

Select Detailed options

Minimum Value: []

Maximum Value: []

Value: []

Done Discard

Create New Option(s) under Variable - Numeric Type

Runtime UEFI Variable Creation: Implementation Snaps VIII

Create Option

Variable name	anotherVar	Option Unique Id	Option Name	Type	Offset	Size	Default Value	Current Value	Description	Edit
Guid	0x{9455d9-0x8740-0x11ea-0xb8-0xc6-0x00-0x0a-0x0d-0x33-0x10}									
Attributes	7 (0x7)									
Is_exist	False									
Size(0x0)	0 (0x0)									
Option Type	reserved									
Name	ReservedSpace									
Description	Reserved Space within the Nvar									
Size(0x1)	1									
Offset(0x0)	0									

Select this type to create reserved space for future use

Create Reserved Space for future use under Variable



Runtime UEFI Variable Creation: Implementation Snaps IX

This XML file does not appear to have any style information associated with it. The document tree is shown below.

```
<SYSTEM>
  <!-- Generated by [REDACTED] -->
  <Nvar name="Option" Guid="0xbff24c08-0x873c-0x11ea-0x98-0xde-0x00-0x0a-0xcd-0x33-0x38-0x26" Attributes="0x7" Size="0x2">
    <knob name="revision" setupType="numeric" default="0x1" CurrentVal="0x7" size="0x1" offset="0x0" description="Revision number" min="0x0" max="0xff"/>
    <knob name="SubOption" setupType="oneOf" default="0x4" CurrentVal="0x4" size="0x1" offset="0x1" description="option descriptions..."/>
    <options>
      <option text="option 1" value="0x0"/>
      <option text="option 2" value="0x1"/>
      <option text="option 3" value="0x2"/>
      <option text="option 4" value="0x3"/>
      <option text="option 5" value="0x4"/>
    </options>
  </knob>
  </Nvar>
  <Nvar name="demo" Guid="0x0003f07e-0x82f7-0x11ea-0x8e-0x6c-0x00-0x0a-0xcd-0x33-0x38-0x26" Attributes="0x7" Size="0xb">
    <knob name="oneVar" setupType="checkbox" default="0x0" CurrentVal="0x0" size="0x1" offset="0x0" description="descript"/>
    <knob name="ReservedSpace" setupType="reserved" default="0x1" CurrentVal="0x1" size="0xa" offset="0x1" description="Reserved Space within the Nvar"/>
  </Nvar>
</SYSTEM>
```

Generate XML SUT



Runtime UEFI Variable Creation: Overview of GUI Actions

Button	Interpretation
Create Variable	Opens a form to create new Variable
Display Created Variable	lists out created variable
Generate XML	Generate XML from the stored session database
Save XML	Saves the generated XML on the storage device
Save to SUT	Applies the Pending changes action (Create/Delete/Modify) to SUT
View JSON	View the stored session database in the json format



Future Scope

- ▶ Development and testing of individual driver component rather than building the whole BIOS image
- ▶ AI powered Search Engine to enhance the findings of FAQs for relevant existing queries and articles
- ▶ Automating the initial BIOS Environment Setup
- ▶ Platform independent easy installation setup for the framework



Thank You



Gahan Saraiya

7.

18MCEC10

32/32