# Credential Guard: Say Good Bye to Pass the Hash/Ticket Attacks

Junaid Ahmed. Jan<sup>1</sup>

Saudi Arabian Oil Company, Dhahran, Kingdom of Saudi Arabia

DOI: https://doi.org/10.5281/zenodo.7886224

Published Date: 02-May-2023

*Abstract:* This paper provides important aspects of "Credential Guard" - An awesome mitigation to PtH/T Attacks with just few clicks of Group policy configuration.

*Keywords:* Credential Guard, LSAISO, LSASS, PtH Attack, Secure Kernel, VBS Config, Virtualization Based Security, Windows 10-11, Windows Modern Security.

### I. INTRODUCTION

Introduced in Windows 10 Enterprise and Windows Server 2016, Credential Guard uses virtualization-based security to isolate secrets so that only privileged system software can access them. Unauthorized access to these secrets can lead to credential theft attacks, such as Pass-the-Hash or Pass-The-Ticket.

Kerberos, NTLM, and Credential manager isolate secrets by using virtualization-based security. Previous versions of Windows stored secrets in the Local Security Authority (LSA). Prior to Windows 10, the LSA stored secrets used by the operating system in its process memory. With Windows Defender Credential Guard enabled, the LSA process in the operating system talks to a new component called the isolated LSA process that stores and protects those secrets. Data stored by the isolated LSA process is protected using Virtualization-based security and isn't accessible to the rest of the operating system. LSA uses remote procedure calls to communicate with the isolated LSA process.

For security reasons, the isolated LSA process doesn't host any device drivers. Instead, it only hosts a small subset of operating system binaries that are needed for security and nothing else. All of these binaries are signed with a certificate that is trusted by virtualization-based security and these signatures are validated before launching the file in the protected environment.

When Windows Defender Credential Guard is enabled, NTLMv1, MS-CHAPv2, Digest, and CredSSP can't use the signedin credentials. Thus, single sign-on doesn't work with these protocols. However, applications can prompt for credentials or use credentials stored in the Windows Vault, which aren't protected by Windows Defender Credential Guard with any of these protocols. It is recommended that valuable credentials, such as the sign-in credentials, aren't to be used with any of these protocols. If these protocols must be used by domain or Azure AD users, secondary credentials should be provisioned for these use cases.

When Windows Defender Credential Guard is enabled, Kerberos doesn't allow unconstrained Kerberos delegation or DES encryption, not only for signed-in credentials, but also prompted or saved credentials.

### **II. OVERVIEW**

Here's a high-level overview on how the LSA is isolated by using Virtualization-based security:



https://learn.microsoft.com/en-us/windows/security/identity-protection/credential-guard/credential-guard-how-itworks

### **III. DEEP DIVE**

In this research paper you will see different configurations and associated events and display information.

Firstly, lets us examine a machine without credential guard enabled and see what we can derive from

LSASS on Windows 10 domain joined machine.

On my lab client machine I am using <u>mimikatz</u>tool (BY Benjamin Deply - <u>https://github.com/gentilkiwi</u>) to extract **hashes** from memory (<u>LSASS</u>):

Fig.	Π
- <b>O</b>	

Authentication Id :	0 : 233728 (00000000:00039100)		
Session :	Interactive from 1		
User Name :	administrator		
Domain :	CONTOSO		
Logon Server :	DC		
Logon Time :	5/24/2017 1:18:59 AM		
SID :	5-1-5-21-1469689841-4213604591-3442953207-500		
msv :			
[0000003]	Primary		
* Username	: Administrator		
* Domain	: CONTOSO		
* NTLM	: eaa4bb35b0e582b247335bcbb5dea412		
* SHA1	: e3d927ff20f3b587df63b8388122d49b59d1b36e		
* DPAPI	: 1e19849f813cebb2e907762030a999b2		
tspkg :			
wdigest :			
* Username	: Administrator		
* Domain	: CONTOSO		
* Password	: (null)		
kerberos :			
* Username	: Administrator		
* Domain	: CONTOSO.COM		
* Password	: (null)		
ssp :			
credman :			

In Fig. II we can see NTLM Hash is being displayed and can be utilized for PtH/T attacks.

If you will check **msinfo32** (Start > Run - msinfo32) report you will see following configuration being displayed:

International Journal of Computer Science and Information Technology Research ISSN 2348-120X (online)

Vol. 11, Issue 2, pp: (39-49), Month: April - June 2023, Available at: www.researchpublish.com

Fig. IV

Device Guard Virtualization based security	Not enabled
Device Encryption Support	Reasons for failed a
A hypervisor has been detected. Features required for Hyper-V will not be displayed.	

Device Guard Virtualization based security: Not Enabled

Virtualization -based security services configured: Credential Guard will not show up

Let's now configure credential guard using active directory group policy (In lab setup - Domain Controller is on Windows Server 2016):

Open GPMC - Group Policy Management Configuration Management Console or AGPM - Advanced Group Policy Management MMC (Whatever you are using). Even for testing you can use local GPMC on Windows 10 or Server machine.

Fig. V

### Edit the GPO which is used for configuring Credential Guard

💠 🔿 🚾 🗙 @ 🛛 🖬		
<ul> <li>Group Policy Management</li> <li>✓ A Forest: contoso.com</li> <li>✓ Domains</li> <li>✓ a contoso.com</li> <li>✓ a contoso.com</li> <li>✓ Default Domain Policy</li> <li>✓ Windows 10 /Server 2016 Security Settings</li> </ul>	Windows 10 /Server 2016 S Scope Details Settings Delegati Links Display links in this location: The following sites domains and QU	contoso.com
<ul> <li>Domain Controllers</li> <li>SecureOU</li> <li>Windows 10 /Server 2016 Security Setting</li> <li>Group Policy Objects</li> <li>WMI Filters</li> <li>Starter GPOs</li> <li>Sites</li> <li>Group Policy Modeling</li> <li>Group Policy Results</li> </ul>	Edit Edit Edit Enforced Link Enabled Save Report View New Window from Here Delete Rename Refresh Help	y to the following groups, use

### - Configure the configuration for Credential Guard

Policy Path: Computer Configuration\Administrative Templates\System\Device Guard

Policy Name	Value
Turn On Virtualization Based Security	Enabled

### \* Configurations:

Option	Value
Select Platform Security Level	Secure Boot and DMA protection
Virtualization Based Protection of Code Integrity	Enabled without UEFI Lock
Credential Guard Configuration	Enabled without UEFI Lock

We will discuss UEFI lock later in this post-



- After restarting client machine we will see "Running configuration" in msinfo32 summary:

Fig. VII

Device Guard Virtualization based security	Running
Device Guard Required Security Properties	Base Virtualization Support, Secure Boot, DMA Protection
Device Guard Available Security Properties	Base Virtualization Support, Secure Boot, DMA Protection,
Device Guard Security Services Configured	Credential Guard, Hypervisor enforced Code Integrity
Device Guard Security Services Running	Credential Guard, Hypervisor enforced Code Integrity

Also we can see one additional process called <u>LSAISO</u> under details TAB of Task manager and also as <u>Credential Guard</u> <u>& Key Guard</u> under Processes Tab:

Fig.	VIII
------	------

📧 Lsalso.exe	912	Running	SYSTEM	00	1,25	Credential Guard & Key Guard
Isass.exe	920	Running	SYSTEM	00	4,29	Local Security Authority Process

Fig.	IX
------	----

👰 Task M File Optic	lanager ons View							
Processes	Performance	App history	Startup	Users	Details	Services		
Name	^			<b>3%</b> CPU	6 Mem	8% hory	2% Disk	0% Network
Apps (2 > 🥵 Sn > 🙀 Ta:	) ipping Tool sk Manager			0.5% 0.5%	7.8 9.0	MB C	0.1 MB/s 0 MB/s	0 Mbps 0 Mbps
Backgro	ound proces	ses (17)		0%	1.9	MB	0 MB/s	0 Mbps
O Co	ortana			0%	0.4	мв	0 MB/s	0 Mbps
Cr	edential Guard	& Key Guard		0%	1.0	MB	0 MB/s	0 Mbps

- After running **mimikatz** tool again and this is what we will get from memory:

Fig, X



As we can see in Fig. X there is no hash displayed and we can see an Encrypted Blob. Hence "ENDGAME" for Pass the Hash/Ticket (PtH/T) Attacks.

A peek at Event Viewer will show following informational Events:

### SYSTEM Event ID 153 :

Fig. XI

System Number of events: 2,429							
W Filtered Log: System; Source; Event ID: 153. Number of events: 11							
Level Date and Time Source Event ID Task Category							
() Information	5/16/2017 12:18:16 PM	Kernel-Boot	153	None			
Event 153, Kernel-Boot General Details							
The Virtualization Based S registry configuration wit	iecurity (policies: VBS Enabled, VSM Required, Secure h status STATUS_SUCCESS.	Boot, Jommu Protection, Mmio Nx, Strong MSR Filte	ring, Hvci, Boot Chain Signer Soft E	nforced) is enabled due to VBS			

The Virtualization Based Security (policies: VBS Enabled, VSM Required, Secure Boot, Iommu Protection, Mmio Nx, Strong MSR Filtering, Hvci, Boot Chain Signer Soft Enforced) is enabled due to VBS registry configuration with status STATUS\_SUCCESS.

Application and Services Logs > Microsoft > Windows > DeviceGuard- Event ID 7000

Fig. XII

evel	Date and Time	Source	Event ID	Task Category
Information	5/16/2017 12:24:35 PM	DeviceGuard	7000	None
vent 7000, DeviceGuard				
General Details				

Device Guard successfully processed the Group Policy: Virtualization Based Security = Enabled, Secure Boot = On, DMAProtection = On, Virtualization Based Code Integrity = Enabled, Credential Guard = Enabled, Reboot required = No, Status = 0x0.

- In order to disable the setting, just configure GPO and choose option Disabled (Do not use Not Configured)

International Journal of Computer Science and Information Technology Research ISSN 2348-120X (online) Vol. 11, Issue 2, pp: (39-49), Month: April - June 2023, Available at: <u>www.researchpublish.com</u>

Turn Or	Virtualiz	ation Ba	ased S	ecurity	Prope	rties		?	Х
Setting	Explain	Preced	lence						
ο Τι	um On Virt	ualization	n Base	d Secu	rity				
	t Configur	ed							
	abled								
Dis	abled								_
Sele	ct Platform	n Security	/ Level	l:					
Virtu	alization B	ased Pro	tectior	n of Coo	de Integ	rity:			
						1			
F	lequire UE	EFI Memo	ory Attri	butes 1	Table				
Cred	ential Gua	ard Config	guration	n:					
						1			
Suppo	rted on:	At least	Windo	ws Ser	ver 201	6, Windows	s 10		
Pr	evious Se	tting	1	Next Se	etting				
			Г	ОК		Cancel		Арр	ly

Fig. XIII

- Run **gpupdate/force** command or reboot the Client

After reboot you will see corresponding Event on Machine - <u>Application and Services Logs > Microsoft > Windows ></u> <u>DeviceGuard- Event ID 7000</u>

Fig.	XIV

monnatio	n 5/24/2017 5:40	25 AM De	eviceGuard	7000	None
Event 7000, De	eviceGuard				
General De	tails				
Device Gu Secure Bo Guard = D	ard successfully processed ot = Off, DMA Protection isabled, Reboot required =	the Group Policy: Virt = Off, Virtualization B No, Status = 0x0.	tualization Based Security Based Code Integrity = Dis	/ = Dis abled,	abled, Credential
General De Device Gu Secure Bo Guard = D	etails ard successfully processed ot = Off, DMA Protection isabled, Reboot required =	the Group Policy: Vir Off, Virtualization B No, Status = 0x0.	tualization Based Security Based Code Integrity = Dis	/ = Dis abled,	abled, Creder

### **Configuration 2 : With UEFI Lock**

Systems which support UEFI Secure Boot maintain an internal security database within UEFI Authenticated Variables. These variables are typically stored in erasable read/write memory with hardware protection against modification by unauthorized parties

http://apps.insyde.com/app/HELP/SecureBootCheckup/UEFI%20Secure%20Boot%20Checkup.html?GeneralUEFIVariab les.html

### International Journal of Computer Science and Information Technology Research ISSN 2348-120X (online)

Vol. 11, Issue 2, pp: (39-49), Month: April - June 2023, Available at: www.researchpublish.com

Fig. XV

	nep				
Group Policy Management ✓ À Forest: contoso.com ✓ Domains ✓ Contoso.com ✓ Default Domain Policy ④ Windows 10 / Server 2016 Security Settings ✓ E Domain Controllers ✓ E SecureOU ↓ Windows 10 / Server 2016 Security Settings ✓ E Group ✓ Wind Windows 10 / Server 2016 Security Settings ✓ E Group ✓ Wind Windows 10 / Server 2016 Security Settings		Windows 10 /Server 2016 Security Settings Scope Details Settings Delegation			
		Furn On Virtualization Based Securi	ity ity	Ben Jacob Cathlorn	
		Not Configured Comment:     Enabled		Previous setung	
Sites     Group Policy     Group Policy     Group Policy	> 😭 Starte File Action View Help > 🛄 Sites 🔶 📫 🖄 🛐 🗐 🖤	Supported on:	At least Wind	ows Server 2016, Windows 10	
	Access-Denie	T Options:		Help:	
	Credentials D	Select Platform Security Level:	2/1	Specifies whether Virtualization	
	Device Guard	Secure Boot and DMA Protection	~	Virtualization Based Security u	
	Device Install.     Device Redire     Disk NV Cach     Disk Outpate	Virtualization Based Protection of Code Enabled with UEFI lock	e Integrity:	Security requires Secure Boot, with the use of DMA Protection hardware support and will only	
	> Distributed C Driver Installa	Credential Guard Configuration: B Enabled with UEFI lock		Virtualization Based Protection	

In Event Viewer we will see System *Event ID 153.* However here we can see some difference:

Fig. XVI

Level		Date and Time	Source	Event ID	Task Category	1
() Informa	ation	5/24/2017 5:40:04 AM	Kernel-Boot	153	None	
Event 153,	Kernel-Boo	ət				×
General	Details					
Virtuali Protect VBS loc	ization-bas tion,Mmio cked config	ed security (policies: VBS Enable Nx, Strong MSR Filtering, Hvci, B guration.	ed, VSM Required, Secure oot Chain Signer Soft En	Boot, lommu forced) is enabl	ed due to	

Virtualization-based security (policies: VBS Enabled,VSM Required,Secure Boot,Iommu Protection,Mmio Nx,Strong MSR Filtering,Hvci,Boot Chain Signer Soft Enforced) is enabled due to VBS locked configuration.

As we can see configuration is set as "*Enabled due to VBS locked configuration*" and in earlier confirulation (Without UEFI lock) it was *enabled due to* "**VBS registry configuration**"

- In MSINFO32 summary following will be displayed:

### Fig. XVII

Device Guard Virtualization based security	Running
Device Guard Required Security Properties	Base Virtualization Support, Secure Boot, DMA Protection
Device Guard Available Security Properties	Base Virtualization Support, Secure Boot, DMA Protection, UEFI Code Readonly
Device Guard Security Services Configured	Credential Guard, Hypervisor enforced Code Integrity
Device Guard Security Services Running	Credential Guard, Hypervisor enforced Code Integrity

So that means if we disable configuration using Group Policy as we did earlier that is not going to work and in this case we need to do following:

- Disable using GPO - choose option Disabled (Do not use Not Configured)

Turn On Virtualization Based Security Properties $\ \ \ \ \ \ \ \ \ \ \ \ \ \ \ \ \ \ \$
Setting Explain Precedence
Turn On Meturian Proved Security
O Not Configured
C Enabled
Disabled
Select Platform Security Level:
$\sim$
Virtualization Based Protection of Code Integrity:
~
Require UEFI Memory Attributes Table
Credential Guard Configuration:
~
Supported on: At least Windows Server 2016, Windows 10
Previous Setting Next Setting
OK Cancel Apply

Fig. XVIII

- We need to run following commands on elevated command prompt :

mountvol X: /s

copy %WINDIR%\System32\SecConfig.efi X:\EFI\Microsoft\Boot\SecConfig.efi /Y

bcdedit /create {0cb3b571-2f2e-4343-a879-d86a476d7215} /d "DebugTool" /application osloader

bcdedit /set {0cb3b571-2f2e-4343-a879-d86a476d7215} path "\EFI\Microsoft\Boot\SecConfig.efi"

bcdedit /set {bootmgr} bootsequence {0cb3b571-2f2e-4343-a879-d86a476d7215}

bcdedit /set {0cb3b571-2f2e-4343-a879-d86a476d7215} loadoptions DISABLE-LSA-ISO,DISABLE-VBS

bcdedit /set {0cb3b571-2f2e-4343-a879-d86a476d7215} device partition=X:

mountvol X: /d

Fig. XIX



Link : https://docs.microsoft.com/en-us/windows/access-protection/credential-guard/credential-guard-manage

### ISSN 2348-1196 (print) International Journal of Computer Science and Information Technology Research ISSN 2348-120X (online) Vol. 11, Issue 2, pp: (39-49), Month: April - June 2023, Available at: <u>www.researchpublish.com</u>

Here we need to make sure we have both "DISABLE-LSA-ISO,DISABLE-VBS" added in command as GPO configuration which we used had both VBS Protection and Credential selected.

### Above step is very Important in case of UEFI lock because of following:

Systems which support UEFI Secure Boot maintain an internal security database within UEFI Authenticated Variables. These variables are typically stored in erasable read/write memory with hardware protection against modification by unauthorized parties

## Even if we will format the OS drive or use new hard drive this setting will still be there as it is in stored in UEFI memory and only way to delete is to physically attend the machine and follow the steps that are in this paper-

- After commands are executed successfully then Restart PC
- Press F3 on Opt-Out Screen for Credential Guard and then Any key to continue:

Fig. XX



Fig. XXI



- Now press F3 again for Opt-Out for Virtualization Based Security and Any key to continue

Fig. XXII



Fig. XXII



- After reboot, MSINFO Summary will show following:



Device Guard Virtualization based security Not enabled

- Event will also show an event related to Opt-Out UEFI (System Event ID 153)

Level	Date and Time	Source	Event ID	Task Ca			
Information	5/24/2017 6:04:29 AM	Kernel-Boot	153	None			
<ol> <li>Information</li> </ol>	5/24/2017 5:48:32 AM	Kernel-Boot	153	None			
<li>Information</li>	5/24/2017 5:40:04 AM	Kernel-Boot	153	None			
<ol> <li>Information</li> </ol>	5/24/2017 5:36:04 AM	Kernel-Boot	153	None			
<ol> <li>Information</li> </ol>	5/24/2017 5:31:22 AM	Kernel-Boot	153	None			
<							
Event 153, Kernel-Boot							
General Details							
Virtualization-based security (policies: 0) is disabled due to opt-out UEFI variable.							

### Fig. XXIV

Virtualization-based security (policies: 0) is disabled due to opt-out UEFI variable.

- For Disabling VBS in *Virtual Machine*, following PowerShell command needs to executed on Host machine:

### Set-VMSecurity -VMName <VMName> -VirtualizationBasedSecurityOptOut \$true

### **IV. CONCLUSION**

This research paper is intended to provide high level summary of Credential Guard the one of the important security features of modern Windows Operating systems. Credential Guard provides robust protection against Pass the Hash attacks.

### REFERENCES

- [1] Credential Guard https://learn.microsoft.com/en-us/windows/security/identity-protection/credential-guard/ credential-guard-how-it-works
- [2] Prerequisites for Credential Guard: https://learn.microsoft.com/en-us/windows/security/identity-protection/ credential-guard/credential-guard-requirements?source=recommendations
- [3] Security Subsystem Architecture: https://learn.microsoft.com/en-us/previous-versions/windows/it-pro/windows-2000-server/cc961760(v=technet.10)?redirectedfrom=MSDN
- [4] Secure Boot : https://learn.microsoft.com/en-us/windows-hardware/design/device-experiences/oem-secure-boot
- [5] PtH Mitigation: https://download.microsoft.com/download/7/7/a/77abc5bd-8320-41af-863c-6ecfb10cb4b9/ mitigating-pass-the-hash-attacks-and-other-credential-theft-version-2.pdf