black hat EUROPE 2018

DECEMBER 3-6, 2018

EXCEL LONDON / UNITED KINGDOM

Cutting Edge

Microsoft Browser Security — From People Who Owned It

Chuanda Ding (@FlowerCode_)

Zhipeng Huo (@R3dF09)

Wei Wei (@Danny__Wei)

#BHEU / @BLACK HAT EVENTS

Who Are We?

- Tencent
  - Largest social media and entertainment company in China
- Tencent Security Xuanwu Lab
  - Applied and real world security research
- Pwn2Own 2017 Microsoft Edge Category Winner

Tencent 腾讯

腾讯安全玄武实验室
TENCENT SECURITY XUANWU LAB

Disclaimer

This Talk is Based on

Windows 10 1607 (OS build 14393)

- *Pwn2Own* 2017

Windows 10 Insider Preview Build 17074

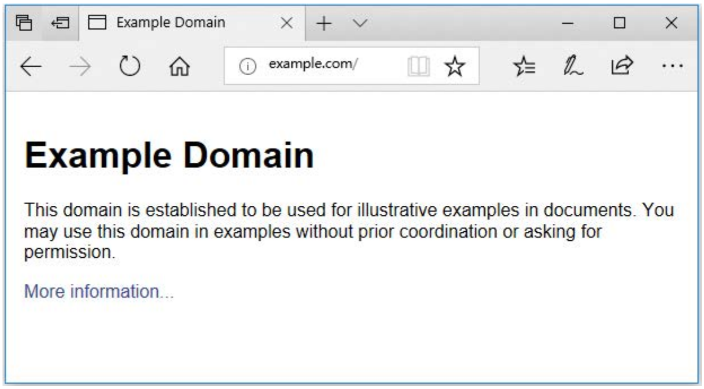
- Vulnerabilities reported to MSRC

Agenda

- Introduction
- Edge Startup and Privilege Separation
- Edge Inter-Process Communication
- Edge Vulnerabilities
  - 1 Real bug used in Pwn2Own 2017
  - 2 New bugs prepared for Pwn2Own 2018

Microsoft Edge

- The default web browser on *Windows 10*
- "The faster, safer way to get things done on the web"
- An *Universal Windows Platform* app
- Target of *Pwn2Own* since 2016



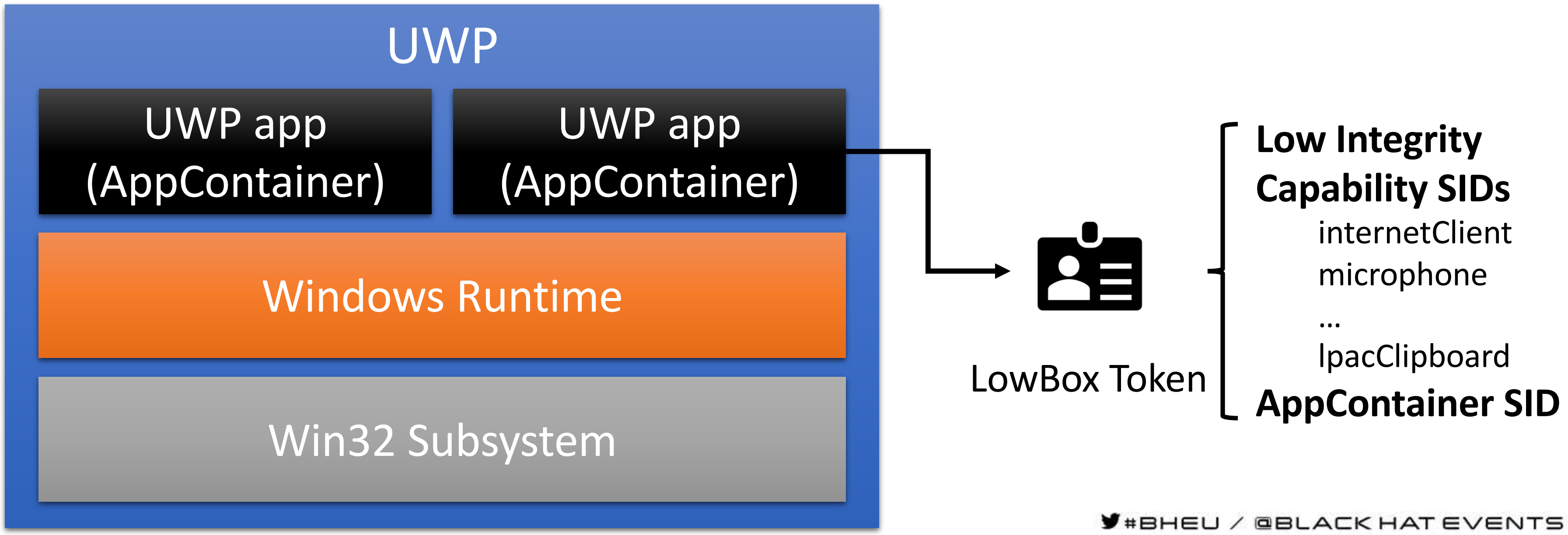
Example Domain

This domain is established to be used for illustrative examples in documents. You may use this domain in examples without prior coordination or asking for permission.

More information...

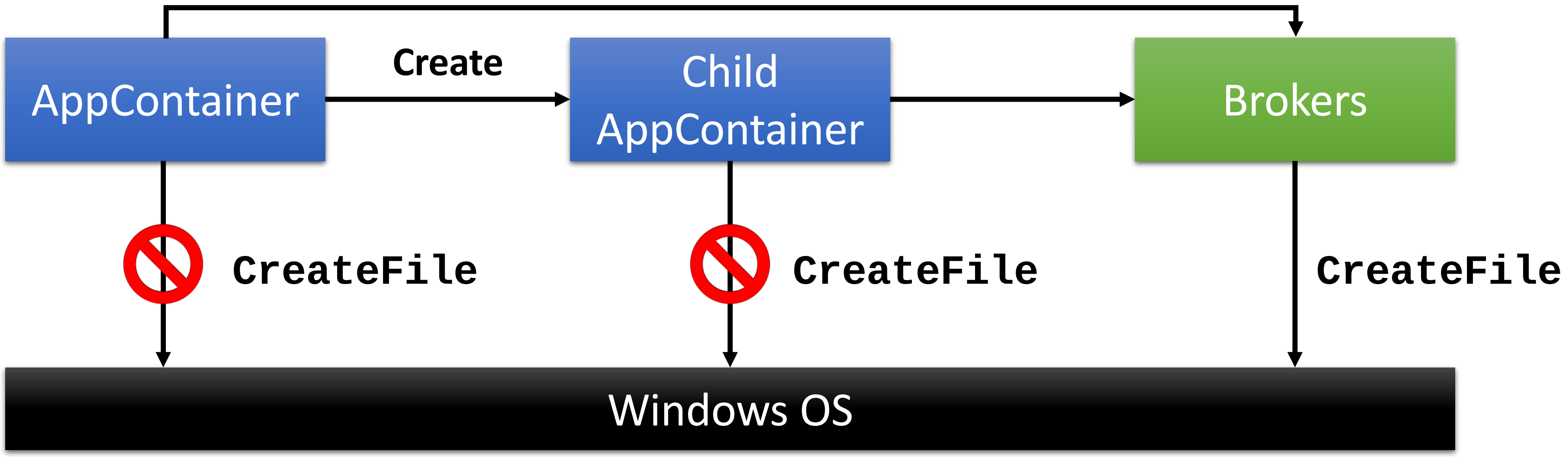
Universal Windows Platform

- UWP apps run in a new type of sandbox called AppContainer
- AppContainer supports several isolation technologies

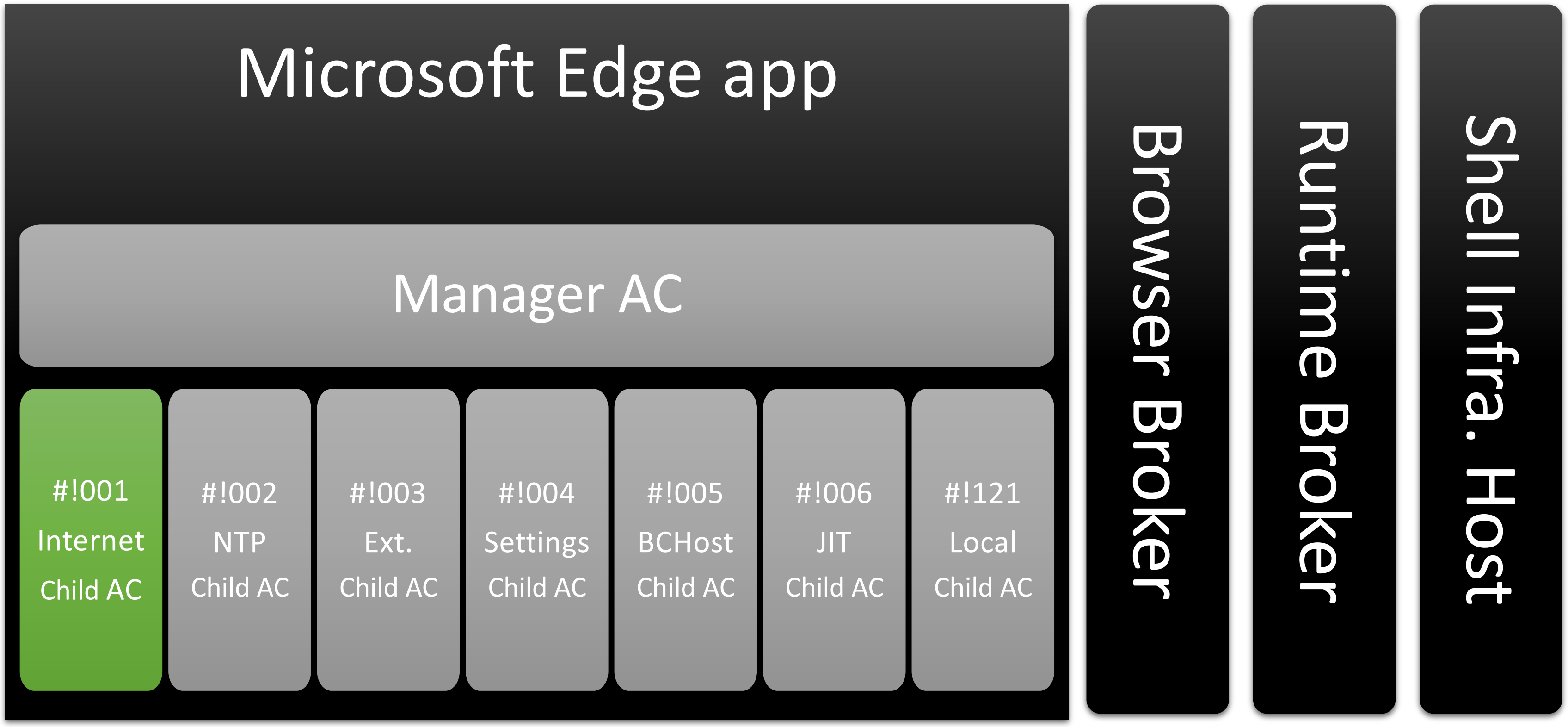


Child AppContainer and Broker

- Child AppContainer is a restricted AppContainer
- AppContainer needs brokers to perform privileged operations

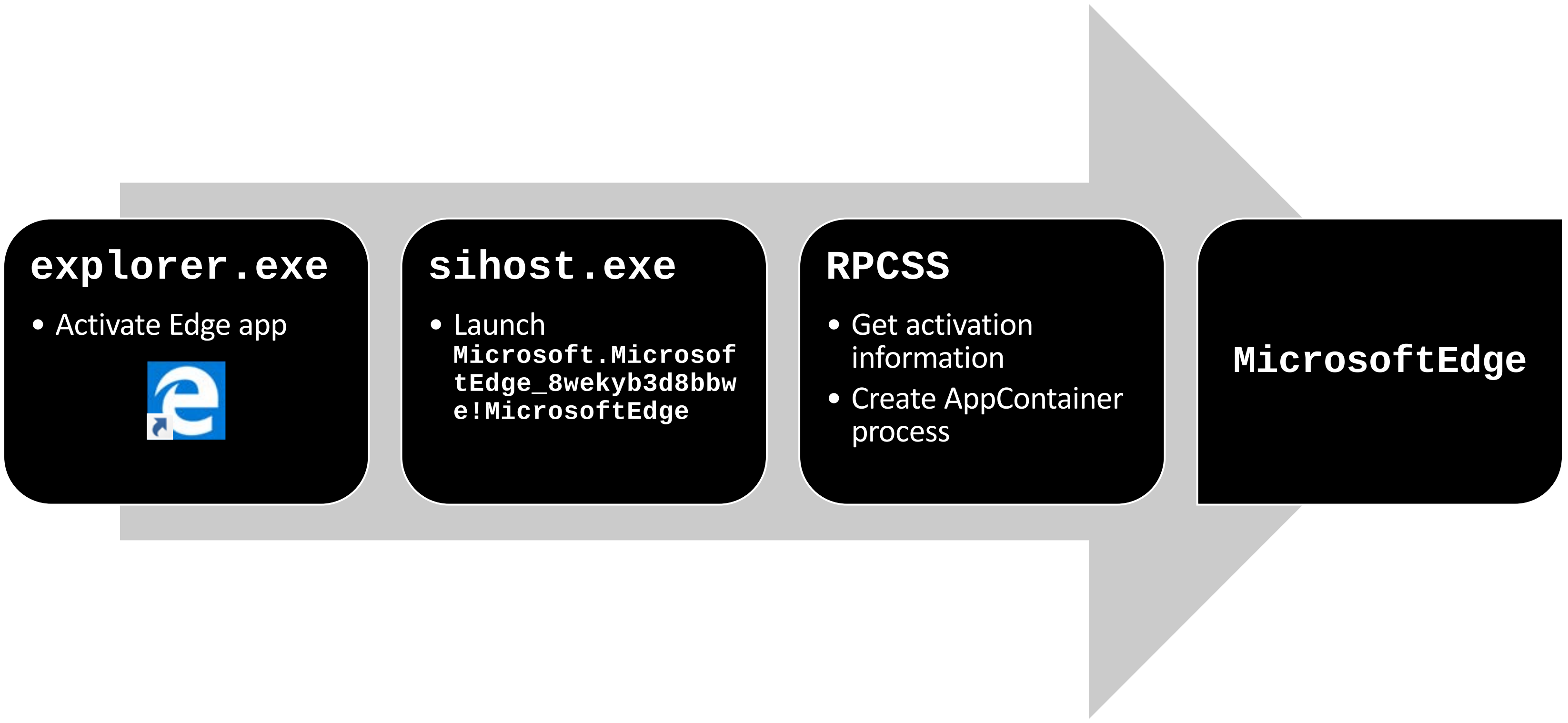


Microsoft Edge Architecture



Process Startup and Privilege Separation

Manager Process Startup



explorer.exe

- Activate Edge app

sihost.exe

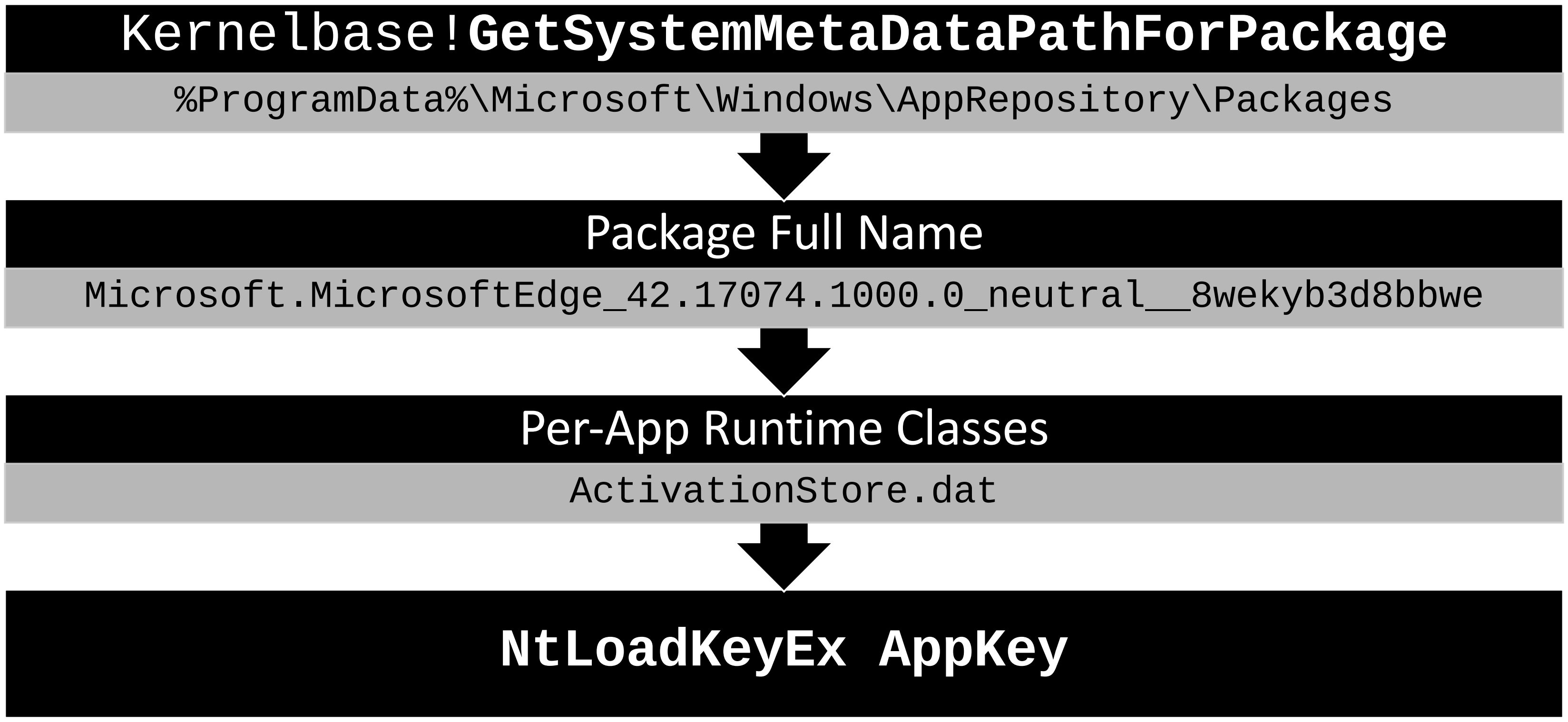
- Launch `Microsoft.MicrosoftEdge_8wekyb3d8bbwe!MicrosoftEdge`

RPCSS

- Get activation information
- Create AppContainer process

MicrosoftEdge

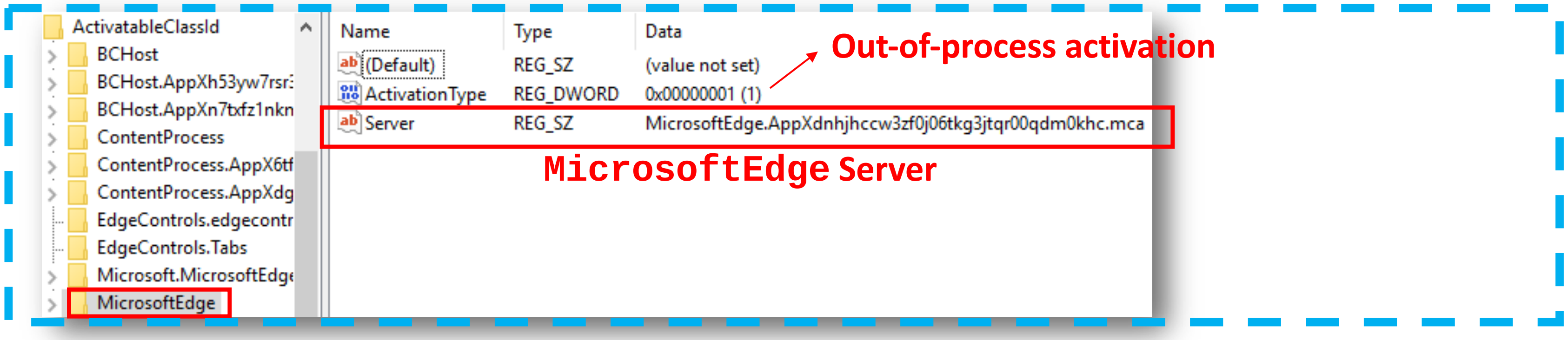
WinRT Runtime Class


Kernelbase!**GetSystemMetaDataPathForPackage**
%ProgramData%\Microsoft\Windows\AppRepository\Packages
Package Full Name
Microsoft.MicrosoftEdge_42.17074.1000.0_neutral__8wekyb3d8bbwe
Per-App Runtime Classes
ActivationStore.dat
NtLoadKeyEx AppKey

black hat EUROPE 2018

Activation Information

Microsoft Edge activation data

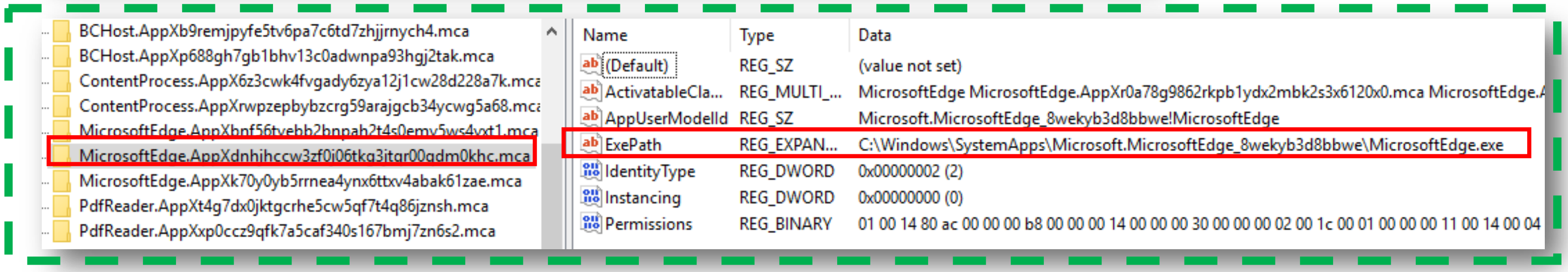


- ActivatableClassId
  - BCHost
  - BCHost.AppXh53yw7rsr
  - BCHost.AppXn7txfz1nkn
  - ContentProcess
  - ContentProcess.AppX6tf
  - ContentProcess.AppXdg
  - EdgeControls.edgecontr
  - EdgeControls.Tabs
  - Microsoft.MicrosoftEdge
  - MicrosoftEdge

Name	Type	Data
(Default)	REG_SZ	(value not set)
ActivationType	REG_DWORD	0x00000001 (1)
Server	REG_SZ	MicrosoftEdge.AppXdnhjhccw3zf0j06tkg3jtqr00qdm0khc.mca

Out-of-process activation

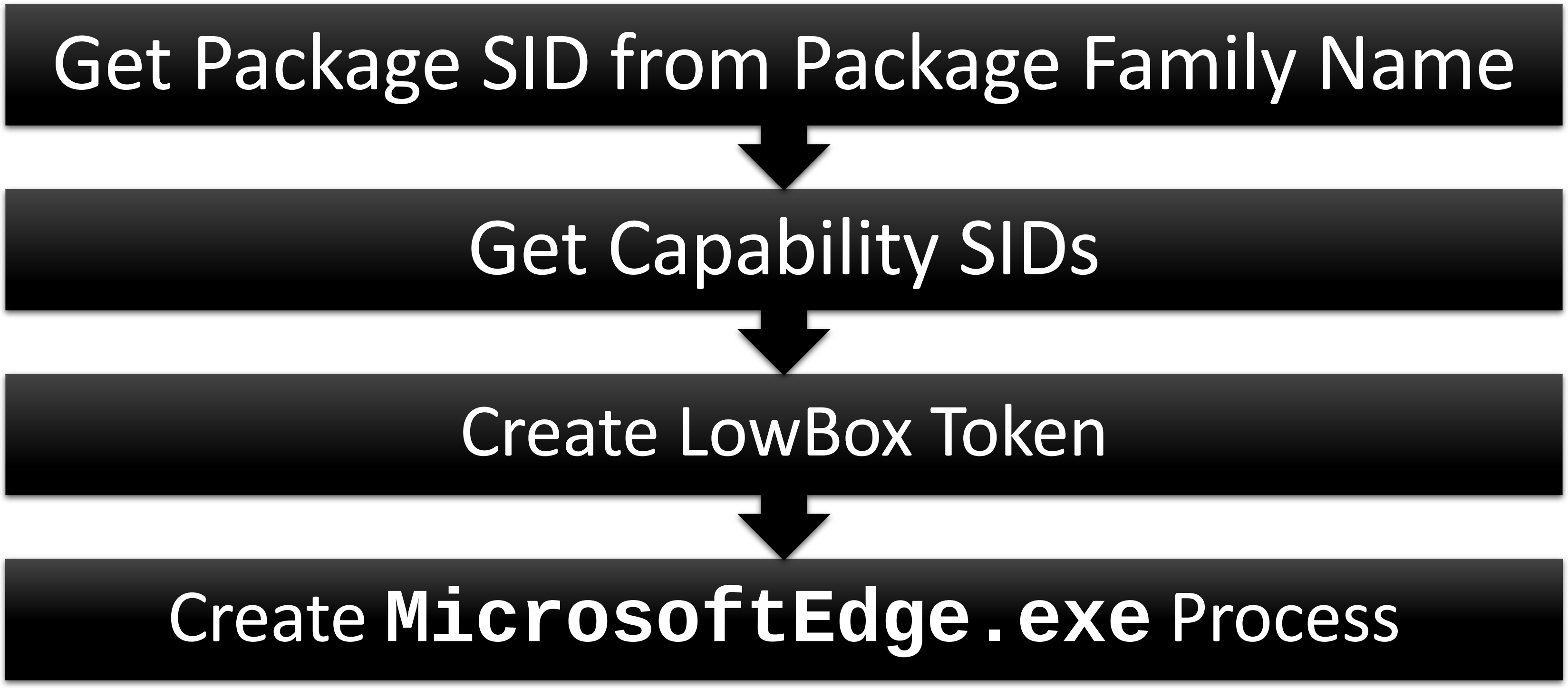
`MicrosoftEdge` Server



- BCHost.AppXb9remjpyfe5tv6pa7c6td7zhjjrnych4.mca
- BCHost.AppXp688gh7gb1bhv13c0adwnpa93hgj2tak.mca
- ContentProcess.AppX6z3cwk4fvgady6zya12j1cw28d228a7k.mca
- ContentProcess.AppXrwpzepbybzcrg59arajgcb34ycwg5a68.mca
- MicrosoftEdge.AppXbnf56tvebb2bnpab2t4s0emv5ws4vxt1.mca
- MicrosoftEdge.AppXdnhjhccw3zf0j06tkg3jtqr00qdm0khc.mca
- MicrosoftEdge.AppXk70y0yb5rrnea4ynx6ttxv4abak61zae.mca
- PdfReader.AppXt4g7dx0jktgcrhe5cw5qf7t4q86jznsh.mca
- PdfReader.AppXxp0ccz9qfk7a5caf340s167bmj7zn6s2.mca

Name	Type	Data
(Default)	REG_SZ	(value not set)
ActivatableCla...	REG_MULTI_...	MicrosoftEdge MicrosoftEdge.AppXr0a78g9862rkpb1ydx2mbk2s3x6120x0.mca MicrosoftEdge.A
AppUserModelId	REG_SZ	Microsoft.MicrosoftEdge_8wekyb3d8bbwe!MicrosoftEdge
ExePath	REG_EXPAN...	C:\Windows\SystemApps\Microsoft.MicrosoftEdge_8wekyb3d8bbwe\MicrosoftEdge.exe
IdentityType	REG_DWORD	0x00000002 (2)
Instancing	REG_DWORD	0x00000000 (0)
Permissions	REG_BINARY	01 00 14 80 ac 00 00 00 b8 00 00 00 14 00 00 00 30 00 00 00 02 00 1c 00 01 00 00 00 11 00 14 00 04

Create AppContainer Process

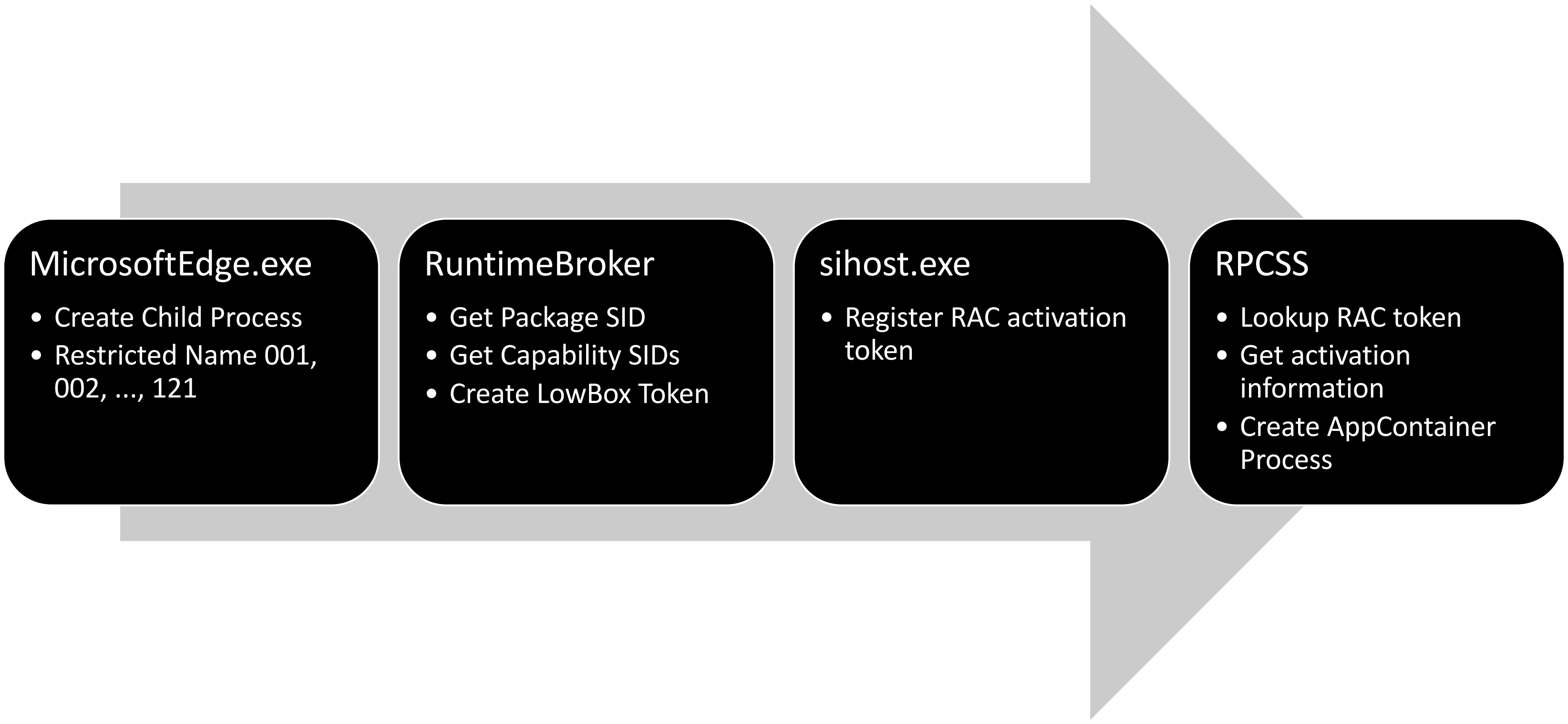

Get Package SID from Package Family Name
Get Capability SIDs
Create LowBox Token
Create **MicrosoftEdge.exe** Process

Manager Process Capabilities

Source of Capability SIDs

- `AppxManifest.xml`
- `PackageSidToPackageCapabilitySid`
- `cellularData`

Content Process Startup



MicrosoftEdge.exe

- Create Child Process
- Restricted Name 001, 002, …, 121

RuntimeBroker

- Get Package SID
- Get Capability SIDs
- Create LowBox Token

sihost.exe

- Register RAC activation token

RPCSS

- Lookup RAC token
- Get activation information
- Create AppContainer Process

Child Process Token and Capabilities

Package SID

- Token of **`MicrosoftEdge.exe`**
- RestrictedName 001, 002, ..., 121
- **`DeriveRestrictedAppContainerSidFromAppContainerSidAndRestrictedName`**

Capability SIDs

- Get Capability SIDs from **`MicrosoftEdge.exe`**

Create new RAC Token in `RuntimeBroker`

Child AppContainer SID

```
S-1-15-2-3624051433-2125758914-1423191267-1740899205-1073925389-
3782572162-737981194
```

- SHA-256 of "**Microsoft.MicrosoftEdge_8wekyb3d8bbwe**"

```
S-1-15-2-1912002900-2594761559-4142726862-4256926629-1688279915-
2739229046-3928706915
```

- SHA-256 of "**001**"

```
S-1-15-2-3624051433-2125758914-1423191267-1740899205-1073925389-
3782572162-737981194-4256926629-1688279915-2739229046-3928706915
```

- Child AC SID for **Microsoft.MicrosoftEdge_8wekyb3d8bbwe/001**

Child Process Capability SIDs

- `edgeIso!`**`GetRACEnumerationFlags`**
- Capability SIDs hardcoded in *Edge*
- **`RestrictedName`** `> 071`
  - **`privateNetworkClientServer`**
  - **`enterpriseAuthentication`**

```
internetClient
sharedUserCertificates
location
microphone
webcam
registryRead
lpacWebPlatform
lpacCom
lpacAppExperience
lpacCryptoServices
lpacIdentityServices
lpacInstrumentation
lpacEnterprisePolicyChangeNotifications
lpacMedia
lpacPnPNotifications
lpacServicesManagement
lpacSessionManagement
lpacPrinting
lpacPayments
lpacClipboard
childWebContent
```

Inter-Process Communications

Edge IPC

Used by renderer, manager and broker

Three types of IPC mechanisms used

- RPC
- COM
- LCIE IPC

RPC

Remote Procedure Call

- ALPC ports, Named pipes, TCP, Hyper-V socket, etc.

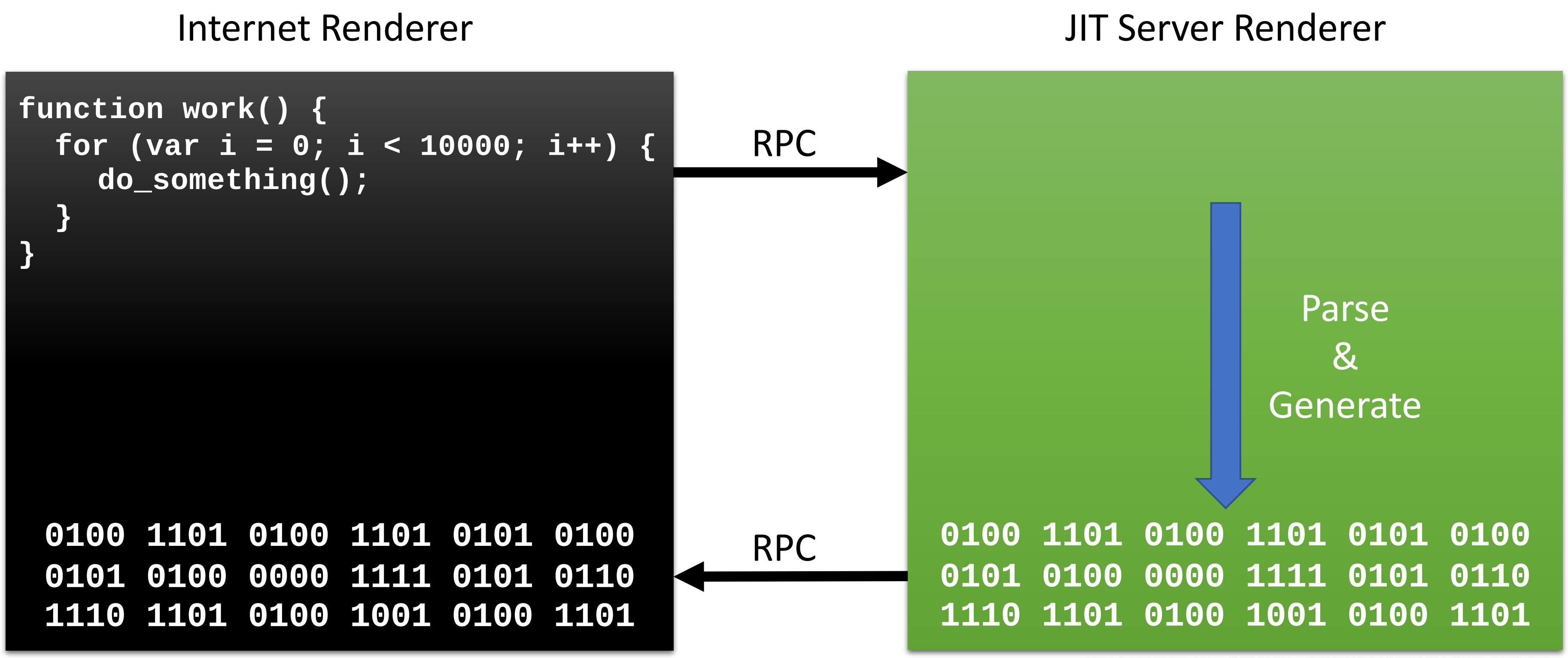
RPC Server

- Listen on endpoints with specified protocol
- Interfaces (Identified by UUID) bind on an endpoint

Security

- Security Descriptor
- Security-callback function

JIT Engine RPC



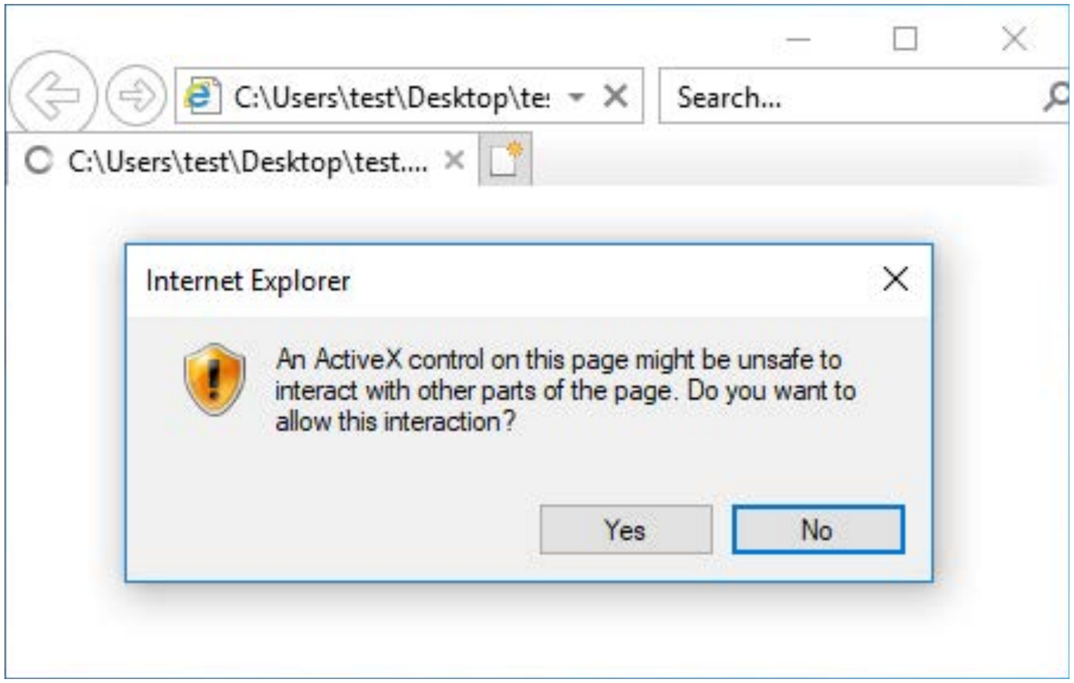
```
function work() {
  for (var i = 0; i < 10000; i++) {
    do_something();
  }
}
```

```
0100 1101 0100 1101 0101 0100
0101 0100 0000 1111 0101 0110
1110 1101 0100 1001 0100 1101
```

```
0100 1101 0100 1101 0101 0100
0101 0100 0000 1111 0101 0110
1110 1101 0100 1001 0100 1101
```

What is COM?

- *ActiveX* is a COM technology

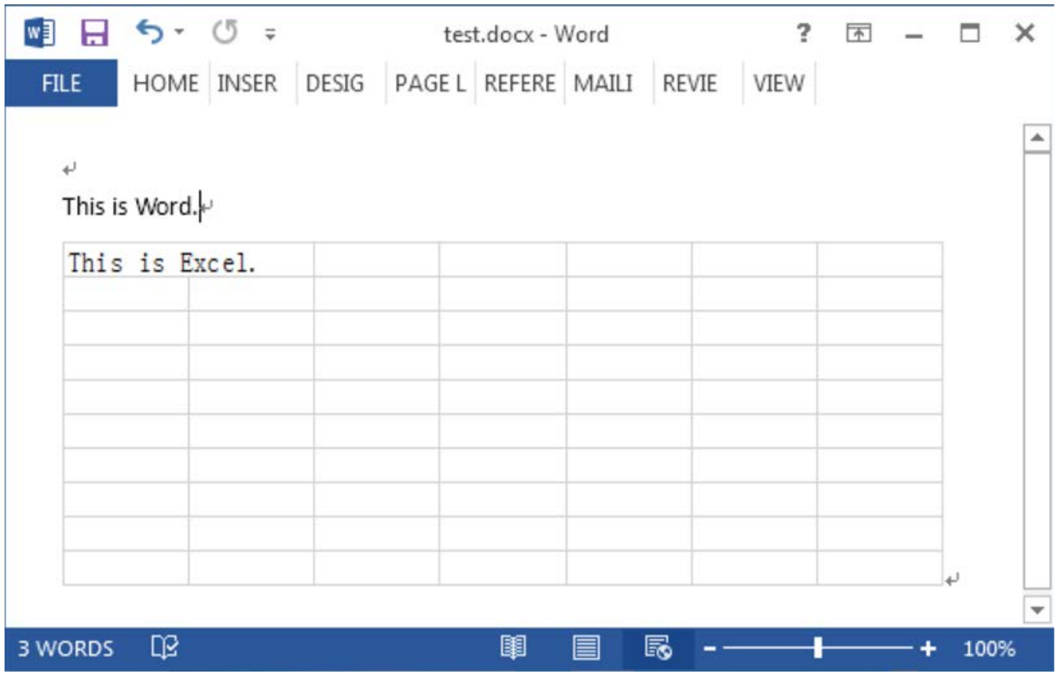


Internet Explorer

An ActiveX control on this page might be unsafe to interact with other parts of the page. Do you want to allow this interaction?

What is COM?

- OLE is also a COM technology



This is Word.

This is Excel.

COM

Component Object Model

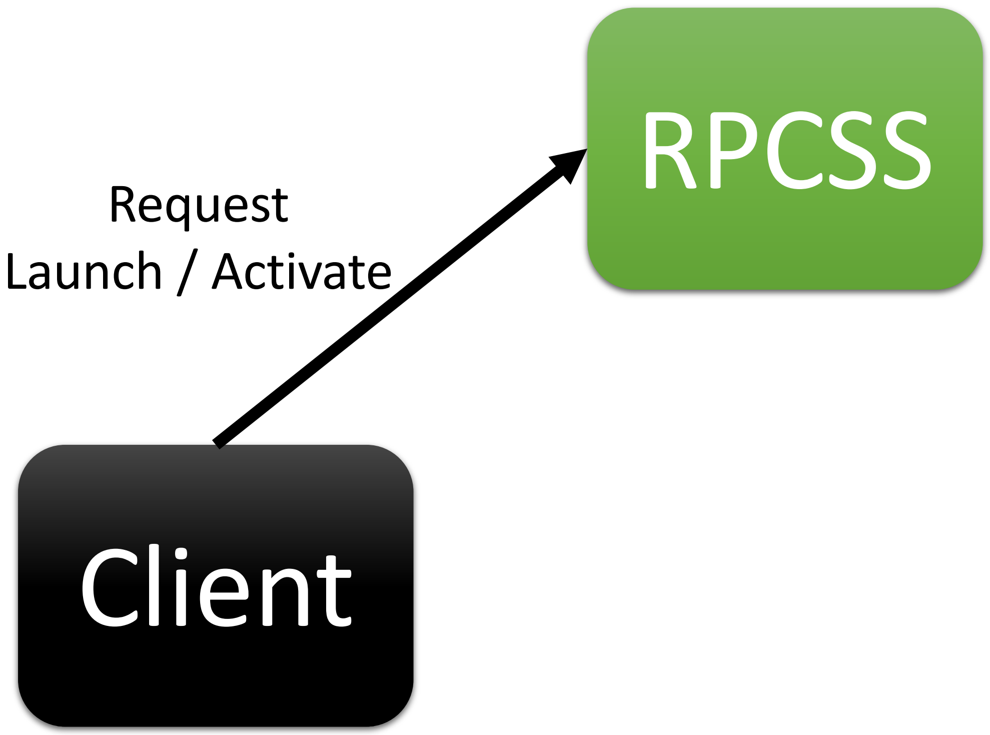
Two Types of COM server

- In-process COM
- Out-of-process COM

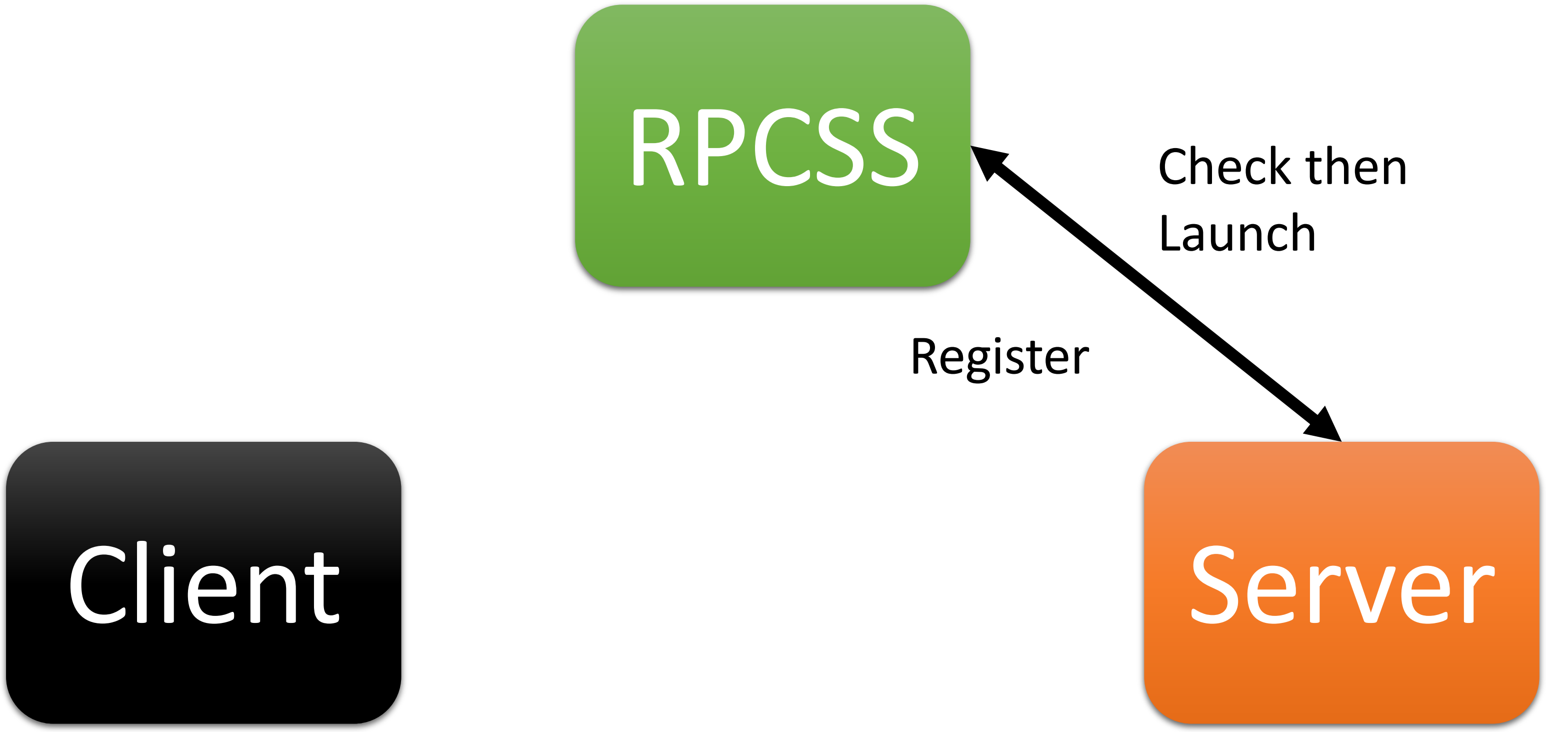
Out-of-process COM

- Runs in a separate process
- Permissions configured by regedit or itself
- Interact through RPC
- Opened up a large attack surface for low-privilege process

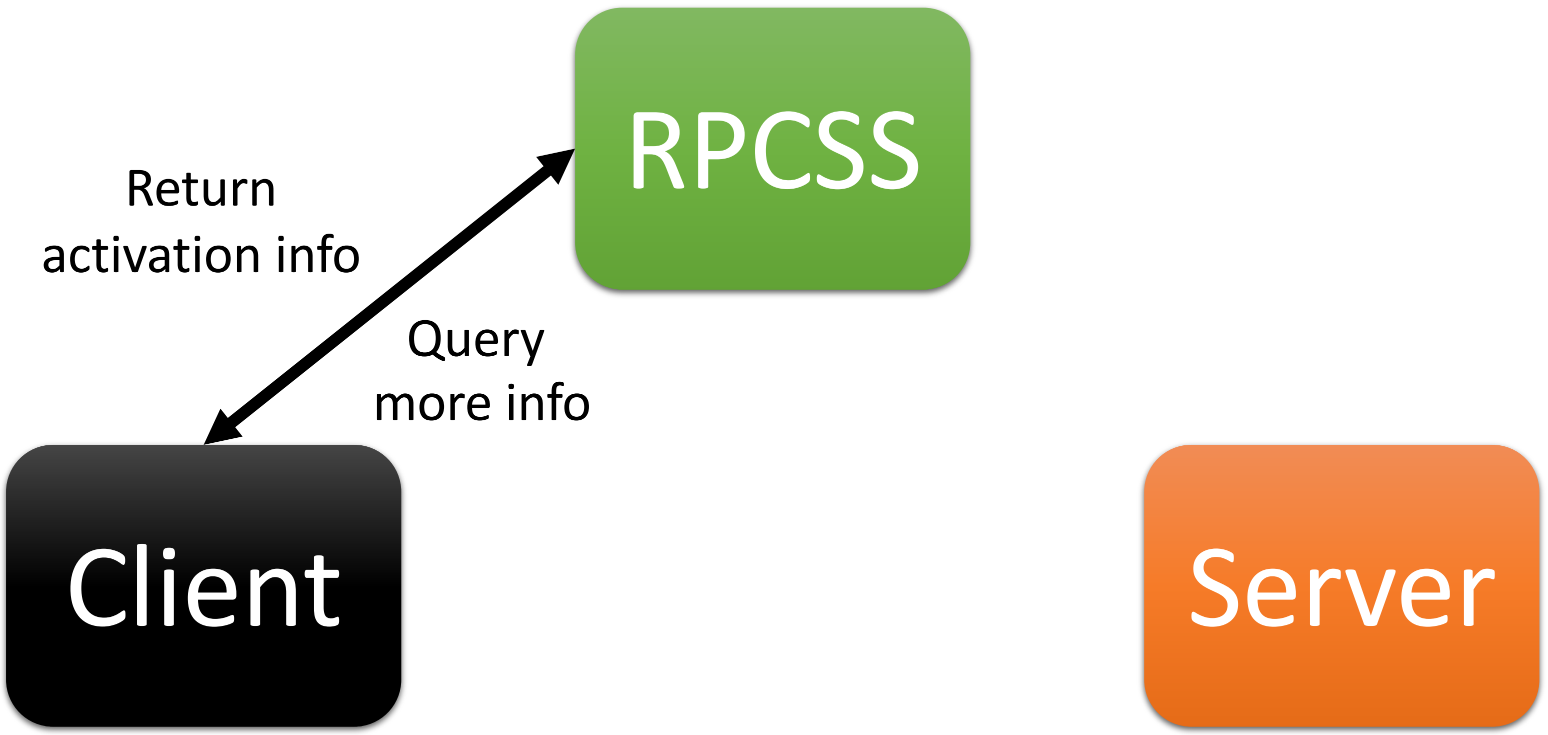
Out-of-Process COM Activation



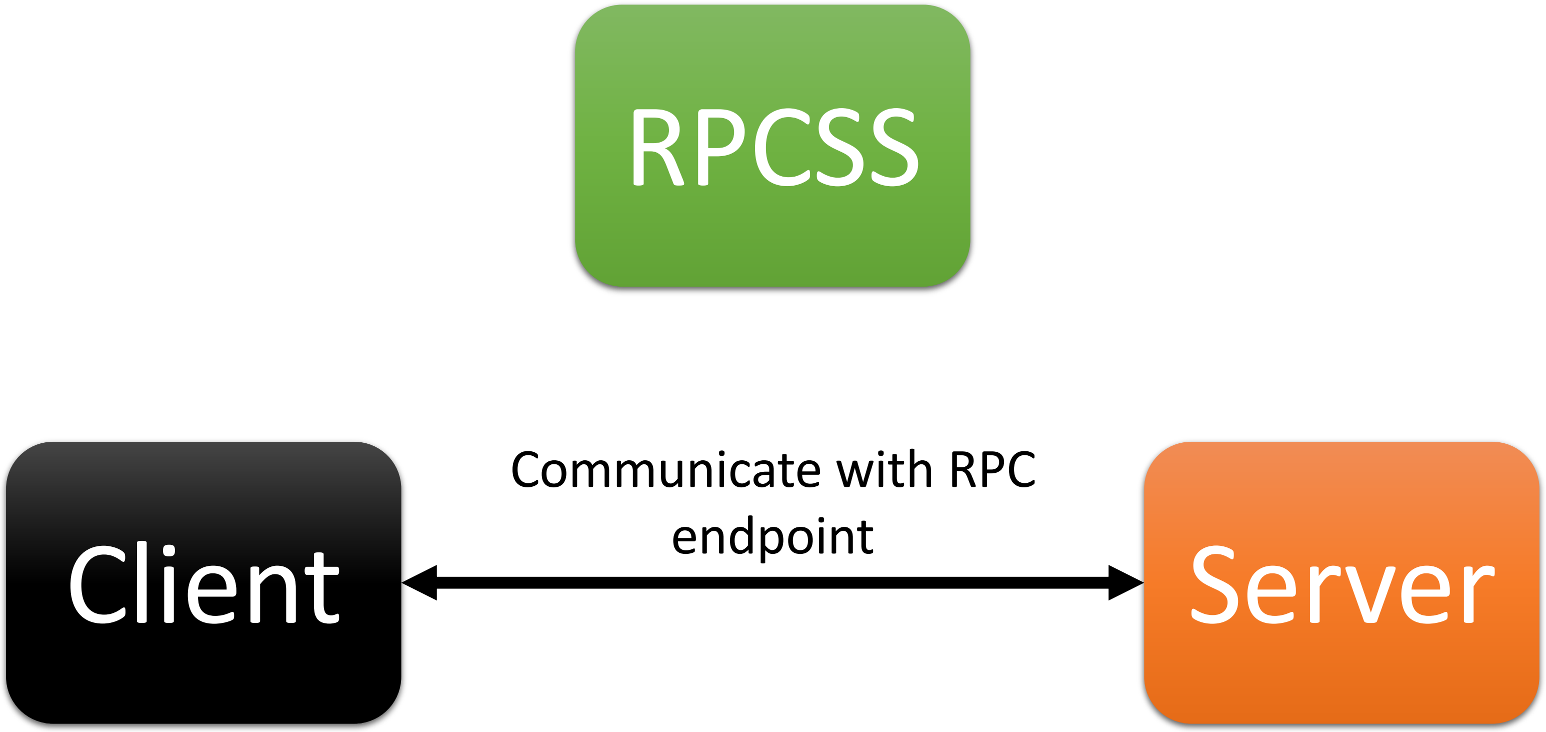
Out-of-Process COM Activation



Out-of-Process COM Activation



Out-of-Process COM Activation



COM Security

System-Wide Security

- Defined in `HKLM\SOFTWARE\Microsoft\Ole`
  - **`DefaultLaunchPermission`**
  - **`DefaultAccessPermission`**

Process-Wide Security

- Defined in `HKLM\SOFTWARE\Classes\AppID\{AppID_GUID}`
  - **`LaunchPermission`**
  - **`AccessPermission`**
- **`CoInitializeSecurity`**
  - COM Server can call it explicitly to override default permission

COM Security

Launch / Activate Permission

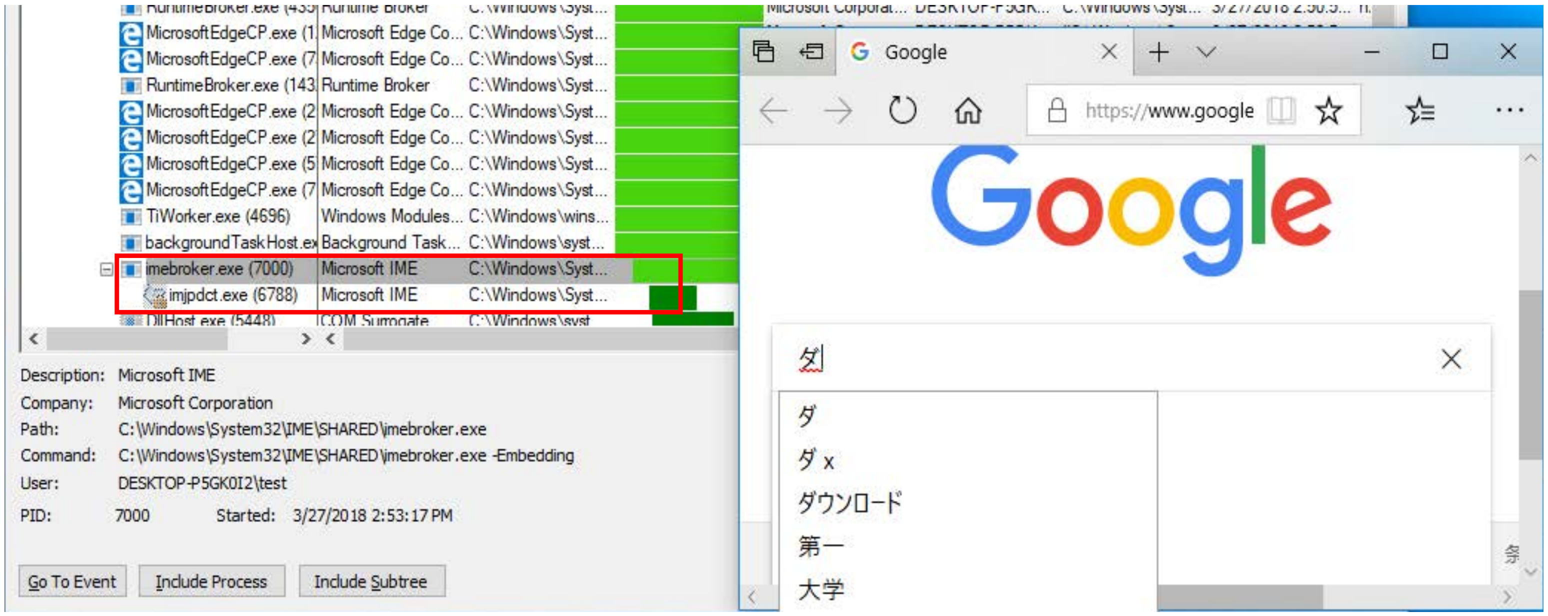
- Checked in **RPCSS** Server
- `rpcss!CClassData::`**`LaunchOrActivationAllowed`**
  - **`Launch`**: Create a new server instance
  - **`Activate`**: Create a new object on an existing server

Access Permission

- Checked in COM runtime at server side
- `combase!`**`ORPCInterfaceSecCallback`**

Dictionary Operation through Out-of-Process COM

- *Edge* uses COM server **`ImeBroker`** to create dictionaries, learn words etc.



```
RuntimeBroker.exe (435 Runtime Broker      C:\Windows\Syst...
MicrosoftEdgeCP.exe (1 Microsoft Edge Co... C:\Windows\Syst...
MicrosoftEdgeCP.exe (7 Microsoft Edge Co... C:\Windows\Syst...
RuntimeBroker.exe (143 Runtime Broker      C:\Windows\Syst...
MicrosoftEdgeCP.exe (2 Microsoft Edge Co... C:\Windows\Syst...
MicrosoftEdgeCP.exe (2 Microsoft Edge Co... C:\Windows\Syst...
MicrosoftEdgeCP.exe (5 Microsoft Edge Co... C:\Windows\Syst...
MicrosoftEdgeCP.exe (7 Microsoft Edge Co... C:\Windows\Syst...
TiWorker.exe (4696)    Windows Modules...  C:\Windows\wins...
backgroundTaskHost.ex  Background Task...  C:\Windows\syst...
imebroker.exe (7000)   Microsoft IME       C:\Windows\Syst...
  imjpdct.exe (6788)   Microsoft IME       C:\Windows\Syst...
DllHost.exe (5448)     COM Surrogate       C:\Windows\syst

Description:  Microsoft IME
Company:      Microsoft Corporation
Path:         C:\Windows\System32\IME\SHARED\imebroker.exe
Command:      C:\Windows\System32\IME\SHARED\imebroker.exe -Embedding
User:         DESKTOP-P5GK0I2\test
PID:          7000        Started:   3/27/2018 2:53:17 PM
```

LCIE IPC

Loosely-Coupled IE introduced in *Internet Explorer* 8

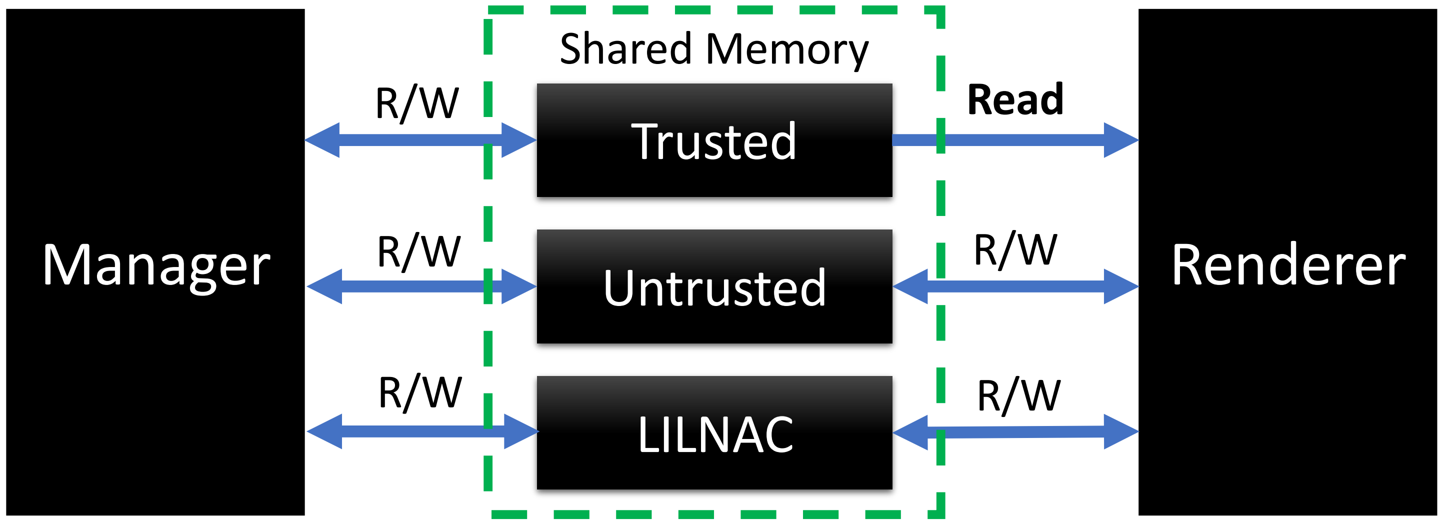
- Isolate tabs (renderers) from the UI frame (manager)

LCIE IPC (Shared Memory IPC)

- Use Section to share data
  - **`CreateFileMapping`** in manager
  - **`OpenFileMapping`** in renderer or broker
  - Three types of sections: **`Trusted`**, **`LILNAC`**, **`Untrusted`**
- **`SetEvent`** to notify target to handle messages in section

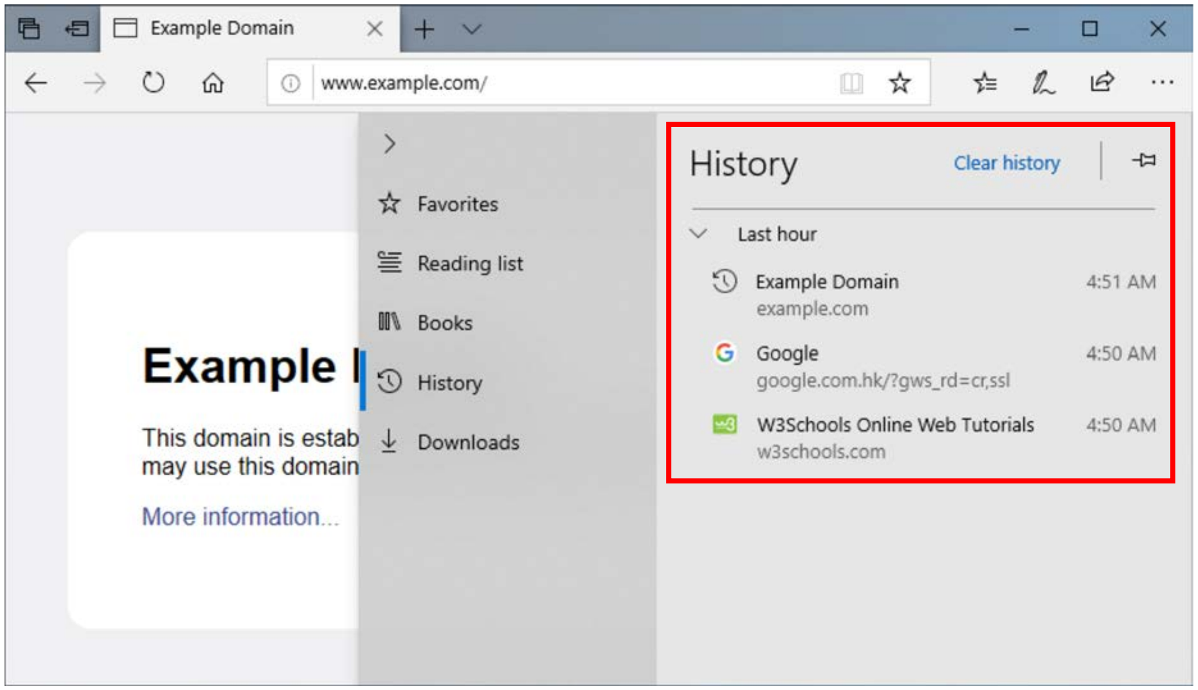
LCIE IPC Message Security

- Message in **Trusted Scope** is trusted
- Manager or Broker may only handle trusted message



Add URL / Favicon to History through LCIE IPC

- Renderer add URL / Favicon to manager's history through LCIE IPC



Example Domain example.com	4:51 AM
Google google.com.hk/?gws_rd=cr,ssl	4:50 AM
W3Schools Online Web Tutorials w3schools.com	4:50 AM

Edge Vulnerabilities

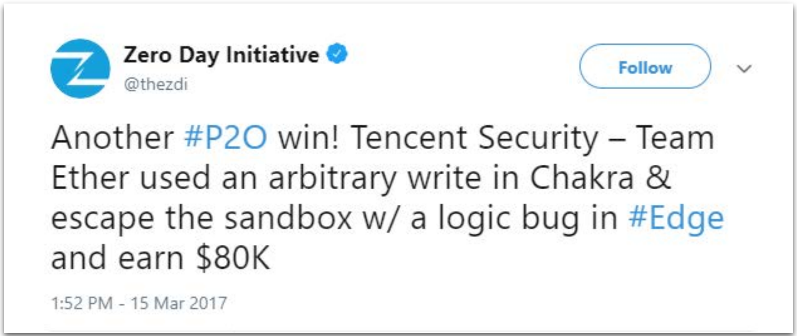
Edge Sandbox Escapes in *Pwn2Own* History

- *Pwn2Own* 2016
  - 1 memory corruption bug and 1 logic bug
- *Pwn2Own* 2017
  - 4 memory corruption bugs and 1 logic bug
- *Pwn2Own* 2018
  - 1 memory corruption bug

Logic bugs are more stable, more generic and lack of attention

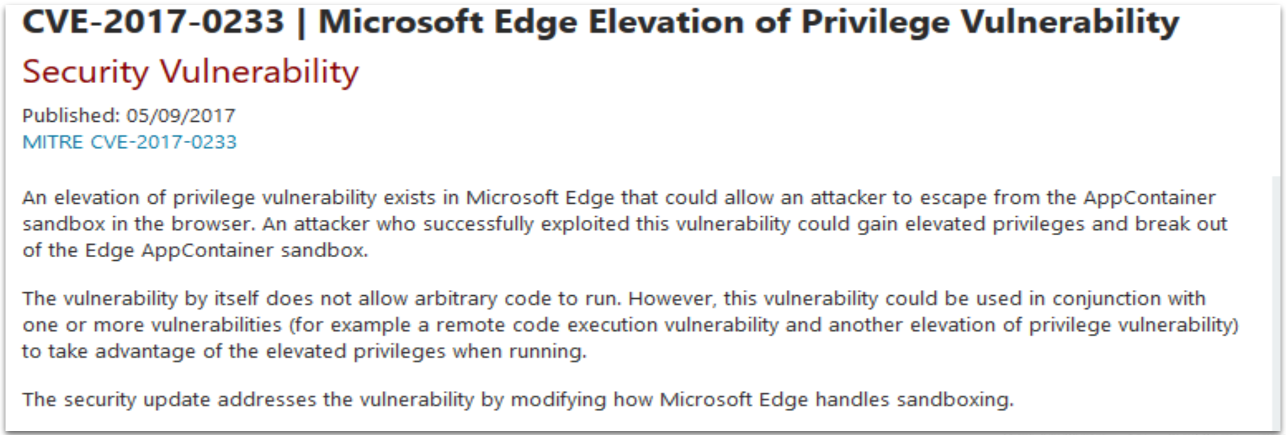
black hat EUROPE 2018

Our Sandbox Escape in *Pwn2Own* 2017


Zero Day Initiative
@thezdi
Follow

Another #P2O win! Tencent Security – Team Ether used an arbitrary write in Chakra & escape the sandbox w/ a logic bug in #Edge and earn $80K

1:52 PM - 15 Mar 2017


CVE-2017-0233 | Microsoft Edge Elevation of Privilege Vulnerability

Security Vulnerability

Published: 05/09/2017
MITRE CVE-2017-0233

An elevation of privilege vulnerability exists in Microsoft Edge that could allow an attacker to escape from the AppContainer sandbox in the browser. An attacker who successfully exploited this vulnerability could gain elevated privileges and break out of the Edge AppContainer sandbox.

The vulnerability by itself does not allow arbitrary code to run. However, this vulnerability could be used in conjunction with one or more vulnerabilities (for example a remote code execution vulnerability and another elevation of privilege vulnerability) to take advantage of the elevated privileges when running.

The security update addresses the vulnerability by modifying how Microsoft Edge handles sandboxing.

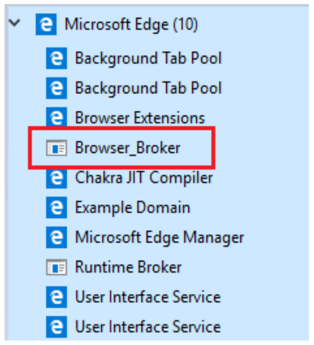
Browser Broker

Browser Broker

- Out-of-process COM Server
- Medium integrity level

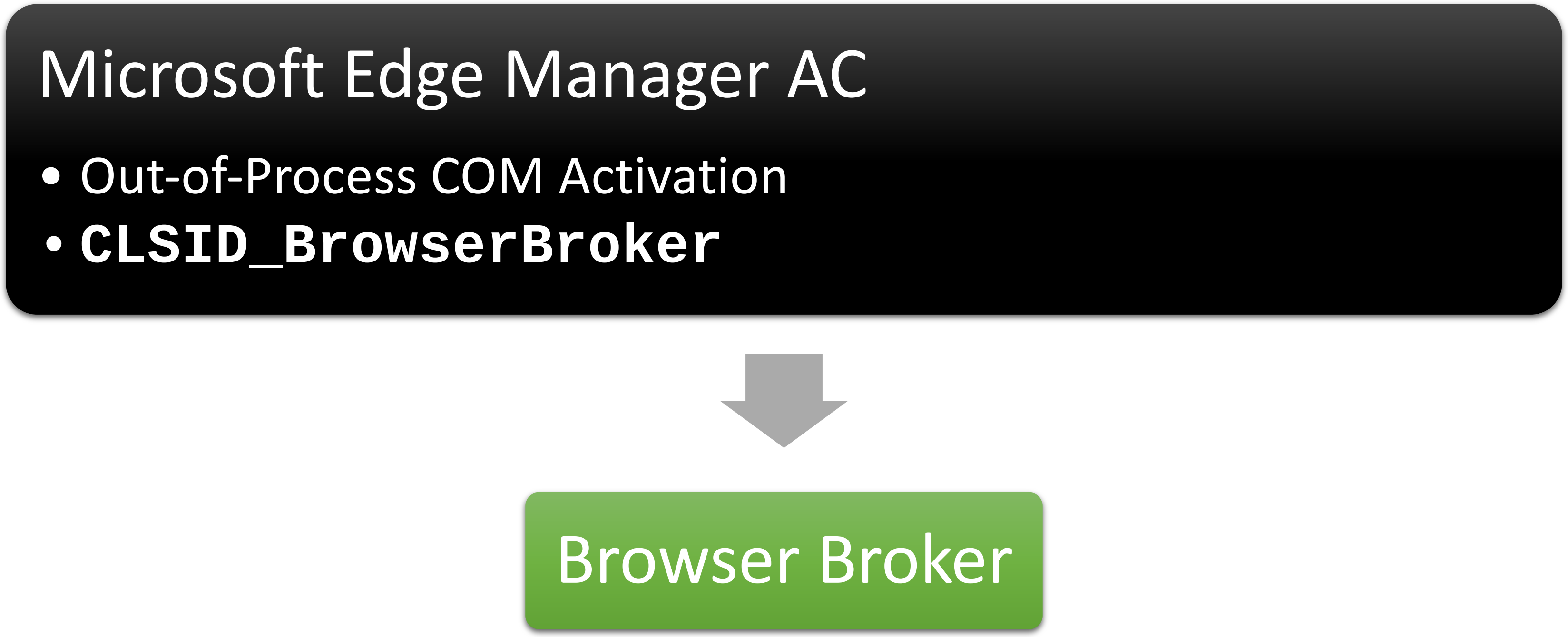
Functionalities

- Methods execute at **Medium Integrity Level**
- e.g. **`LaunchIE`**, **`LaunchInHVSI`**, **`OpenFolder`**, ...



Microsoft Edge (10)
Background Tab Pool
Background Tab Pool
Browser Extensions
Browser_Broker
Chakra JIT Compiler
Example Domain
Microsoft Edge Manager
Runtime Broker
User Interface Service
User Interface Service

Launch Browser Broker in Manager

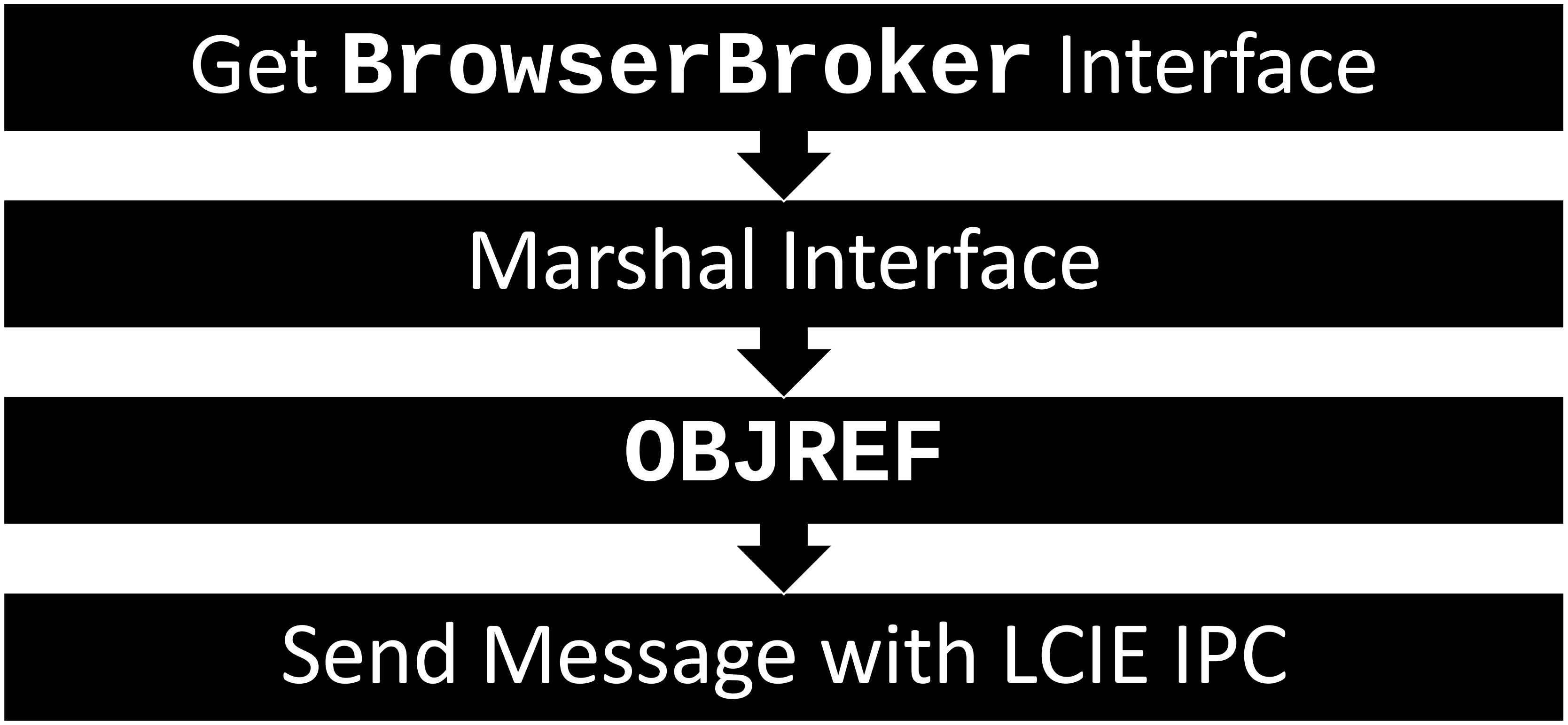


Microsoft Edge Manager AC

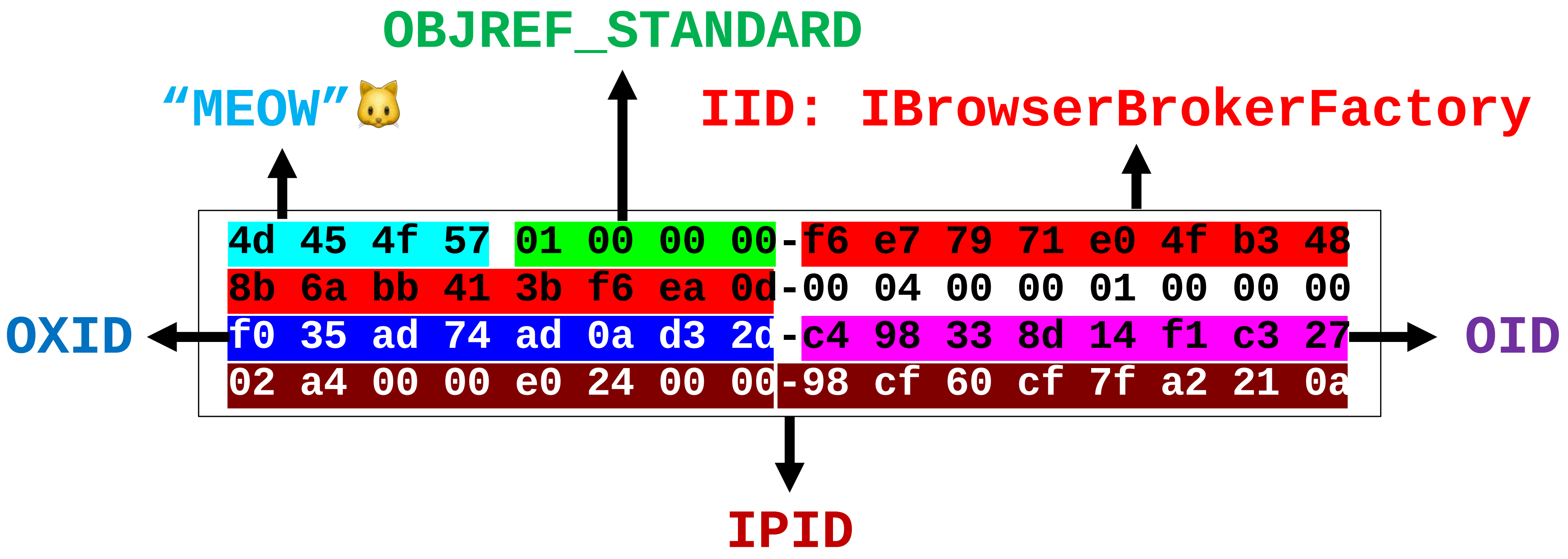
- Out-of-Process COM Activation
- **`CLSID_BrowserBroker`**

Browser Broker

Marshal Interface

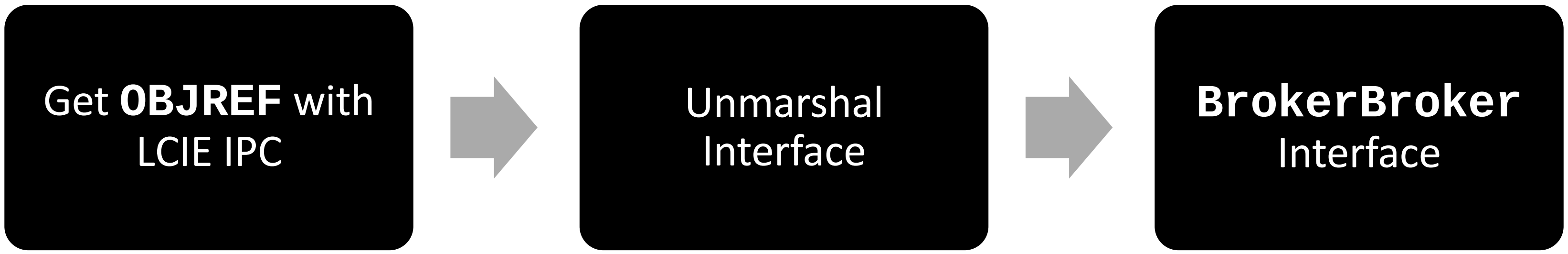


OBJREF



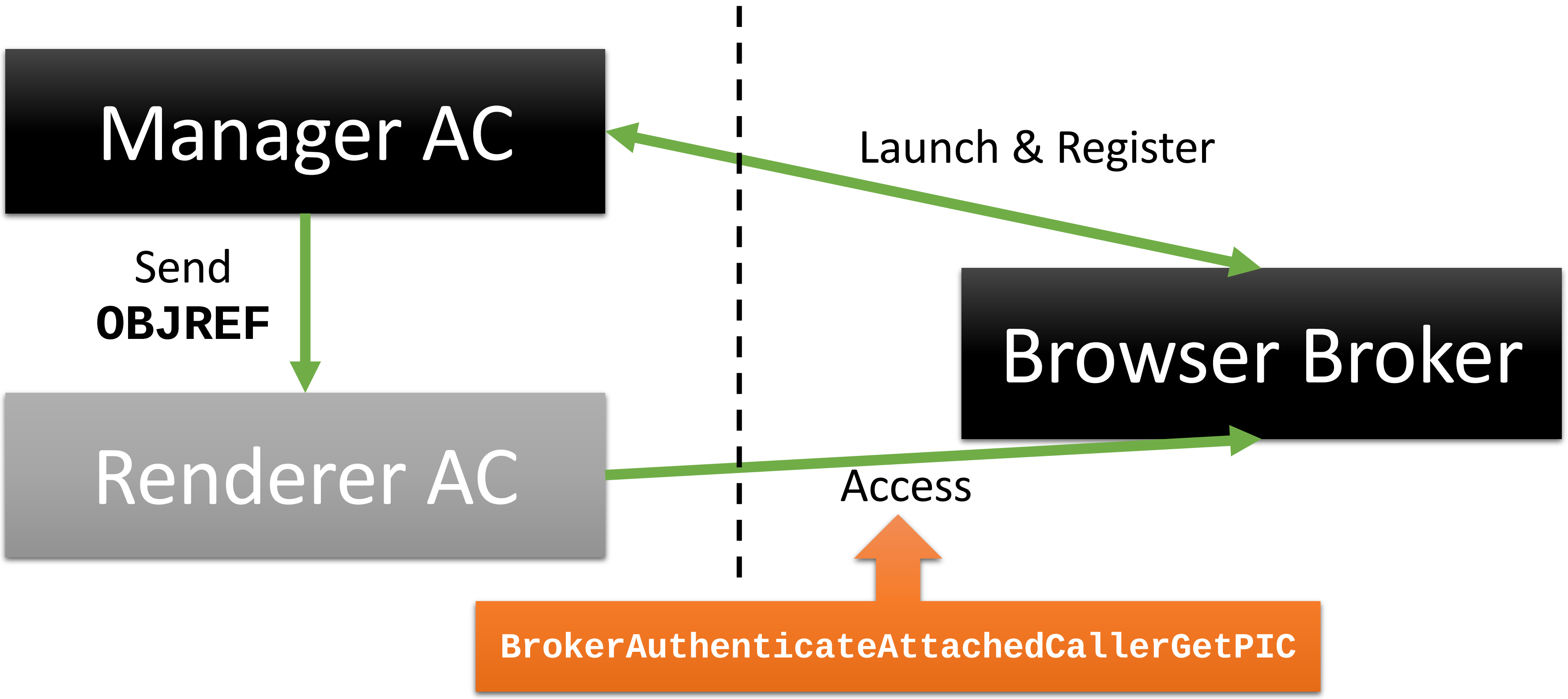
```
4d 45 4f 57  01 00 00 00-f6 e7 79 71 e0 4f b3 48
8b 6a bb 41 3b f6 ea 0d-00 04 00 00 01 00 00 00
f0 35 ad 74 ad 0a d3 2d-c4 98 33 8d 14 f1 c3 27
02 a4 00 00 e0 24 00 00-98 cf 60 cf 7f a2 21 0a
```

Unmarshal Interface



We have a **`BrowserBroker`** interface in content process!

Browser Broker Structure



Edge Child AC Integrity

Process Integrity Level

`IsoIntegrity_PIC_MRAC`	1
`IsoIntegrity_PIC_Dynamic_Low`	7
`IsoIntegrity_PIC_Dynamic_High`	119
`IsoIntegrity_PIC_Intranet_AC`	121
`IsoIntegrity_PIC_Trusted_AC`	122
`IsoIntegrity_PIC_System`	126

Access Check

- 1 Trusted AC only
  - e.g. **`LaunchIE`**
- 2 Everyone
  - e.g. **`CreateBrokerObject`**
- 5 AC except 002
  - e.g. **`AddCredential`**

Trusted AC

Trusted AC is trusted by Browser Broker

Privileged methods check for Trusted AC

SID registered through **`RequestBroker`**

`RequestBroker`

Designed to be called by *Edge* Manager AC

Designed to be called only once

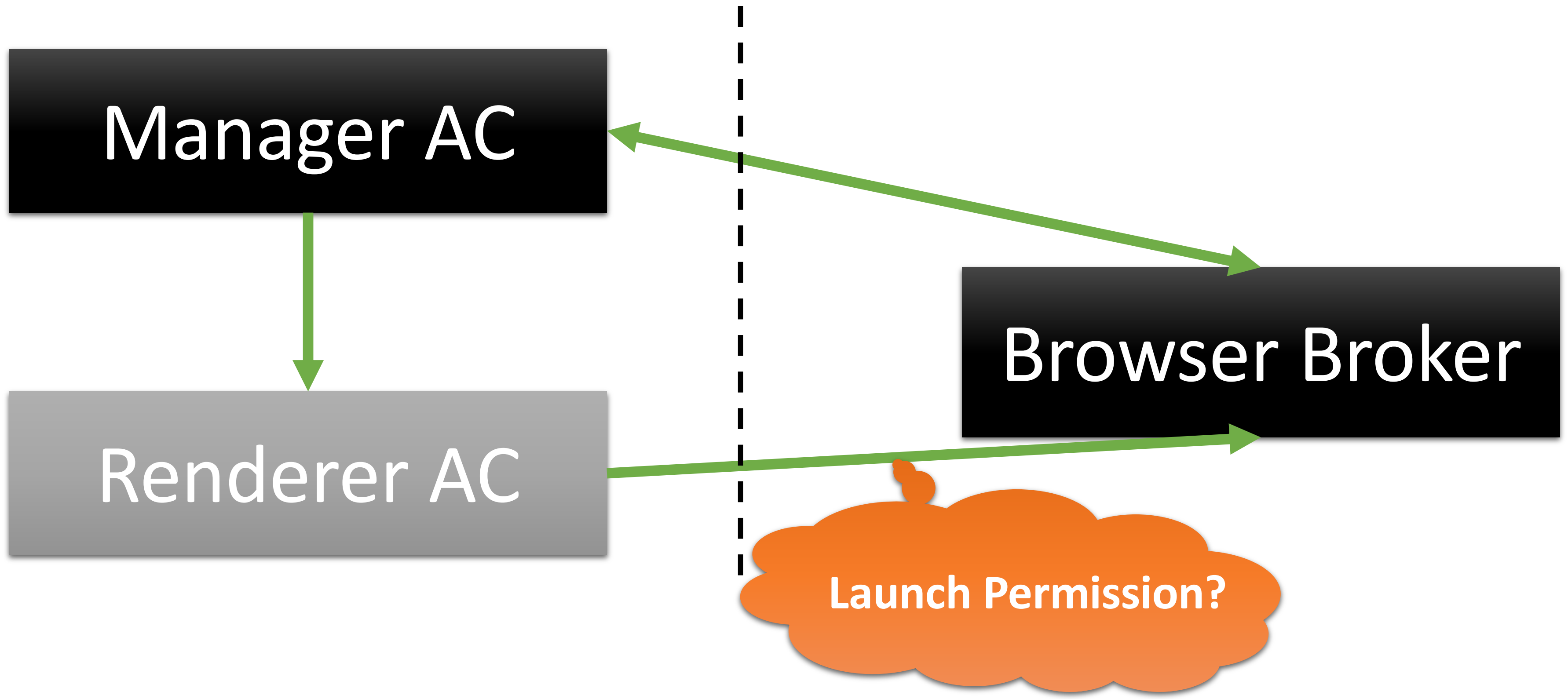
- Cannot call **`RequestBroker`** in child process

Register app identity information

- Application AppContainer SID
- Application Name
- Application Location

Useful, but not accessible in Internet renderer

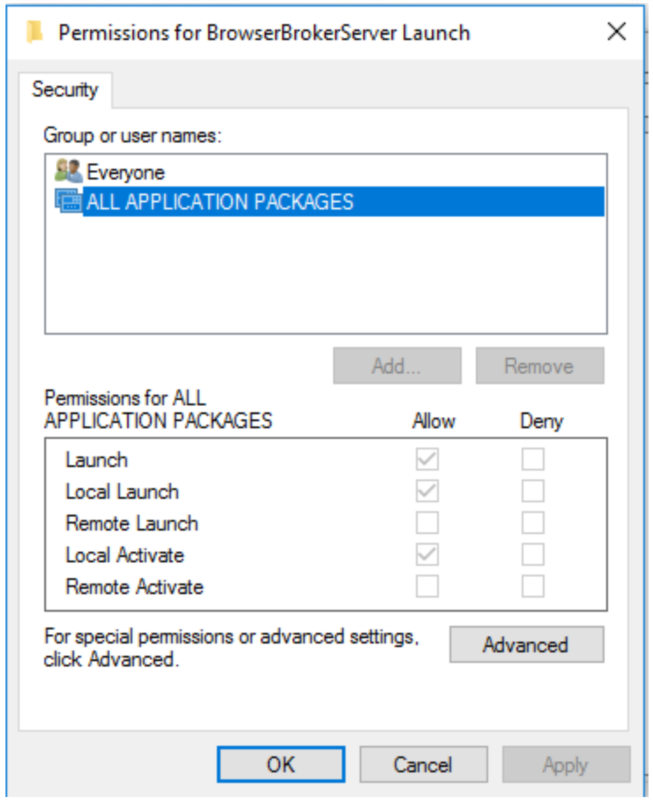
All Roads Lead to Rome



ALL APPLICATION PACKAGES

To allow all AppContainers to access a resource, add the **ALL APPLICATION PACKAGES** SID to the ACL for that resource. This acts like a wildcard.

Implementing an AppContainer


Permissions for BrowserBrokerServer Launch

Security

Group or user names:

Everyone

ALL APPLICATION PACKAGES

Permissions for ALL APPLICATION PACKAGES

	Allow	Deny
Launch	✓	
Local Launch	✓	
Remote Launch		
Local Activate	✓	
Remote Activate		

For special permissions or advanced settings, click Advanced.

CVE-2017-0233

Internet AC launches a new **`BrowserBroker`**

`RequestBroker` with Internet AC SID

Internet AC now becomes a Trusted AC

Full access to all **`BrowserBroker`** methods

Sandbox Escape

```
CBrowserBrokerInstance::WriteClassesOfCategory
   LoadTheSinglePossibleSPFrameDllForThisProcess
      wcscpy(dst, 0x104, AppDir);
      wcscat(dst, 0x104, L"\\eModel.dll");
      LoadLibraryEx(dst, 0, 0x1010);
```

- Register **`AppDir`** through **`RequestBroker`**
- Load our custom **`eModel.dll`** into **`browser_broker.exe`**

Sandbox Escape

Drop custom **`eModel.dll`** to a writable directory

↓

Activate new Browser Broker

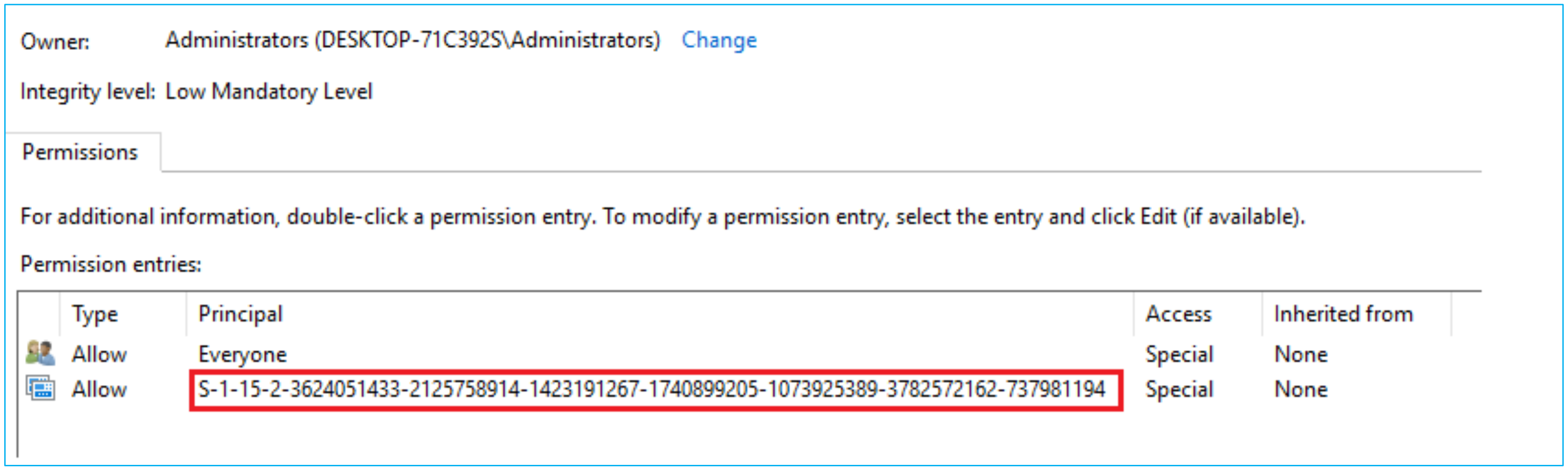
↓

`RequestBroker` with package SID and directory path

↓

`WriteClassesOfCategory`

LaunchPermission



Owner: Administrators (DESKTOP-71C392S\Administrators) Change

Integrity level: Low Mandatory Level

Permissions

For additional information, double-click a permission entry. To modify a permission entry, select the entry and click Edit (if available).

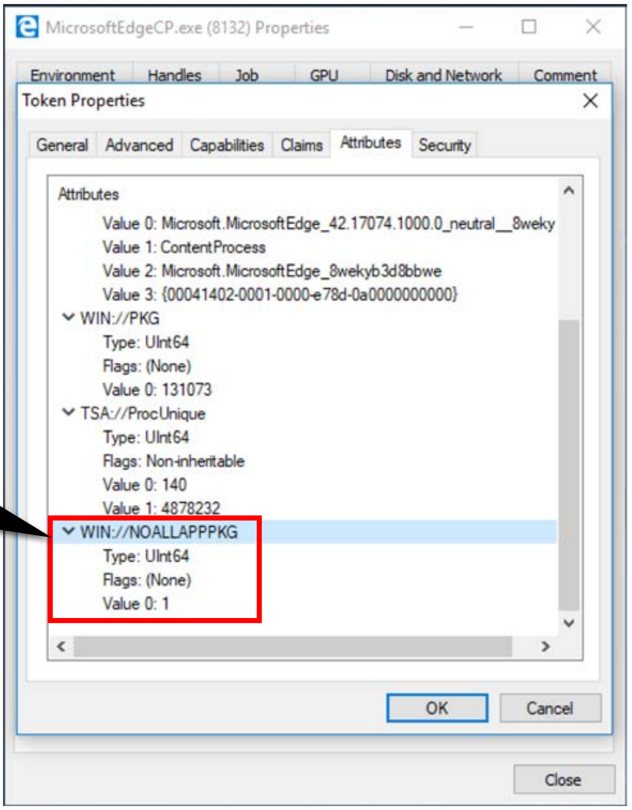
Permission entries:

Type	Principal	Access	Inherited from
Allow	Everyone	Special	None
Allow	S-1-15-2-3624051433-2125758914-1423191267-1740899205-1073925389-3782572162-737981194	Special	None

`BrowserBroker` `LaunchPermission` is limited to Manager process

One Step Forward

Starting from *Windows 10* RS2, renderer cannot access or launch securable objects with **`ALL APPLICATION PACKAGES`** allowed **`ACE`**



MicrosoftEdgeCP.exe (8132) Properties

```
Attributes
    Value 0: Microsoft.MicrosoftEdge_42.17074.1000.0_neutral__8weky
    Value 1: ContentProcess
    Value 2: Microsoft.MicrosoftEdge_8wekyb3d8bbwe
    Value 3: {00041402-0001-0000-e78d-0a0000000000}
  WIN://PKG
    Type: UInt64
    Flags: (None)
    Value 0: 131073
  TSA://ProcUnique
    Type: UInt64
    Flags: Non-inheritable
    Value 0: 140
    Value 1: 4878232
  WIN://NOALLAPPPKG
    Type: UInt64
    Flags: (None)
    Value 0: 1
```

Is This the End?

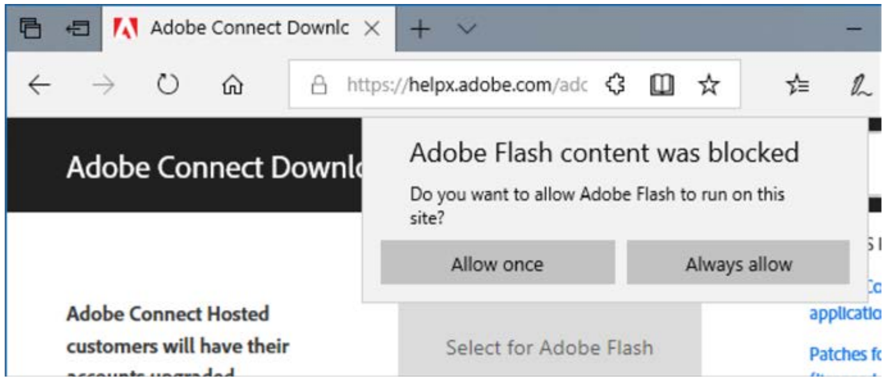
Insert a dramatic pause here.

Adobe Flash

- Led the way for rich content, animations, games, etc.
- Pre-installed starting from *Windows 8*
- No longer supported after 2020

Microsoft Edge Adobe Flash Integration

- Preloaded auto-run whitelist or Click-to-Run
- By default, *Adobe Flash Player* runs in a special renderer called **`BCHost`**


Adobe Connect Downlc

https://helpx.adobe.com/adc

Adobe Connect Downl

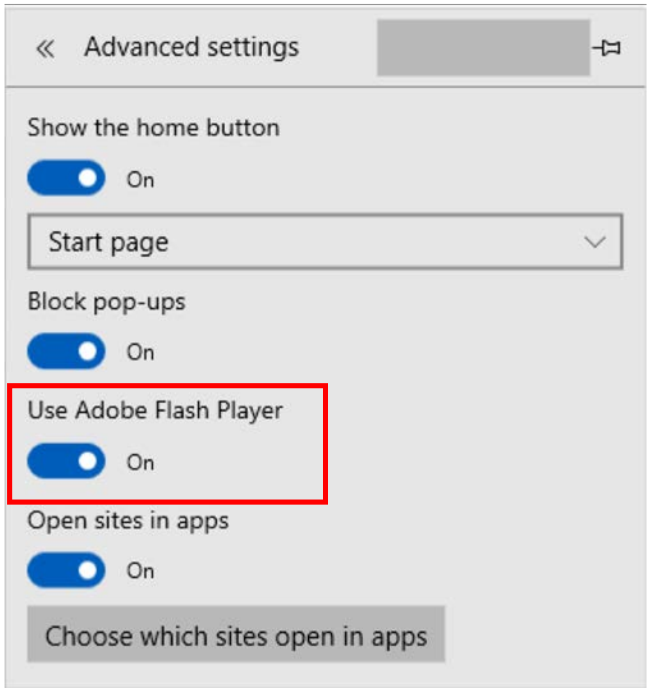
Adobe Flash content was blocked

Do you want to allow Adobe Flash to run on this site?

Allow once | Always allow

Adobe Connect Hosted customers will have their

Select for Adobe Flash


Advanced settings

Show the home button: On

Start page

Block pop-ups: On

Use Adobe Flash Player: On

Open sites in apps: On

Choose which sites open in apps

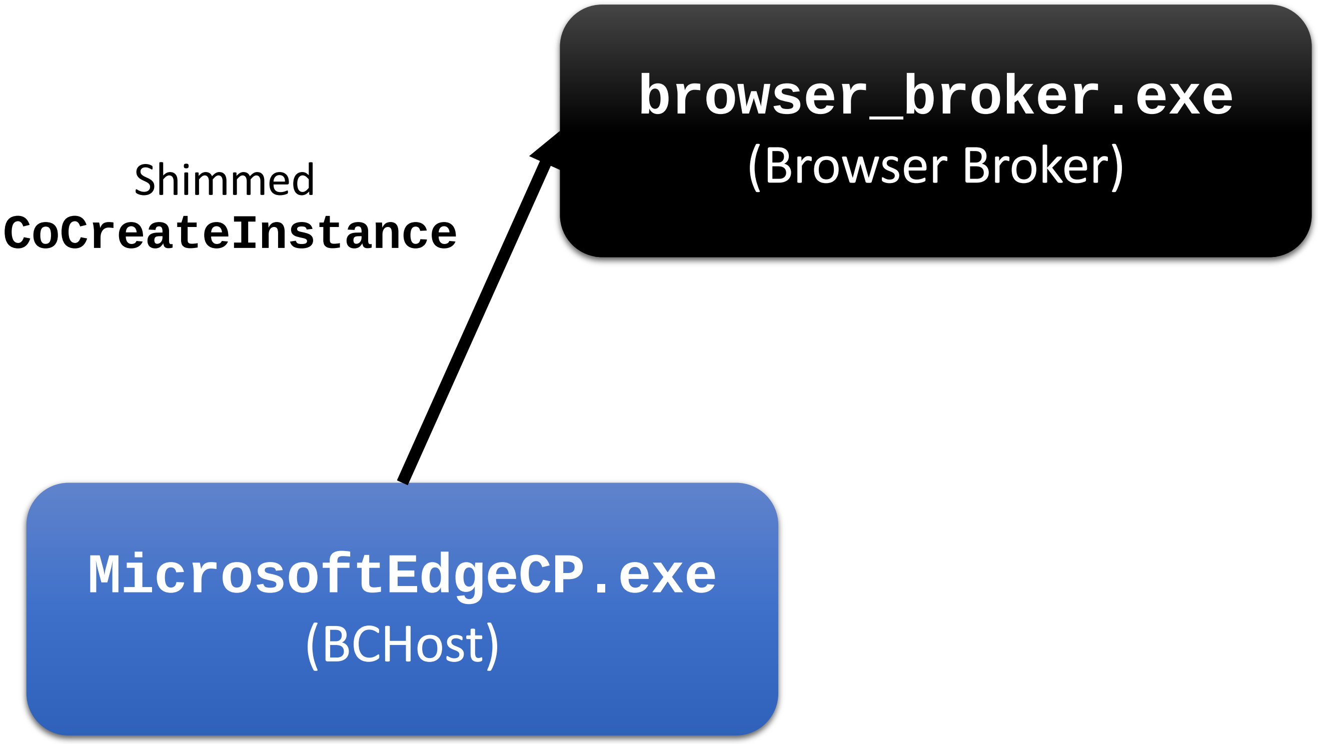
Flash Broker

- Manage *Adobe Flash Player*
- Manage some *Flash* based add-ins
  - *Adobe Connect* Add-in
  - *Microsoft Outlook* Add-in
  - *Cisco Unified Presenter* Add-in
  - etc.
- Opened up another attack surface for *Edge* sandbox

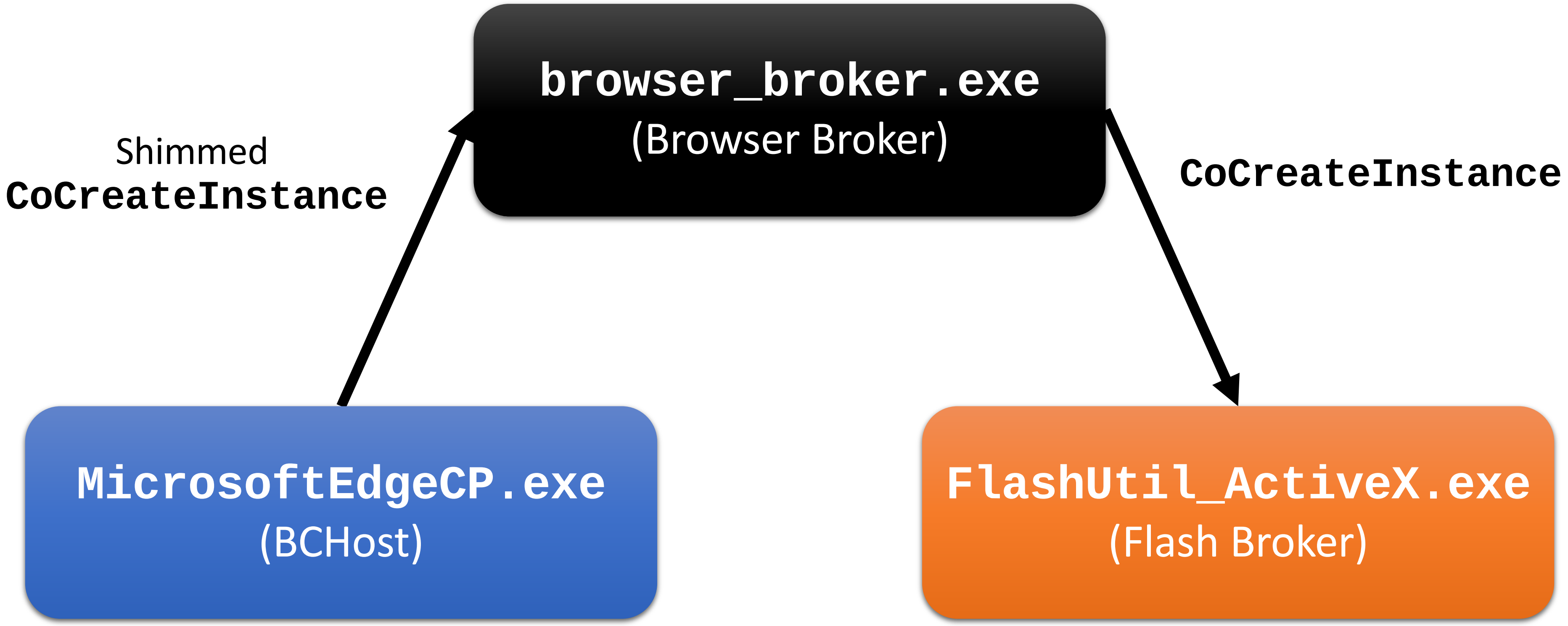
Flash Broker Permissions

- Launch / Activate
  - Renderer does not have permission to launch / activate *Flash* broker
- Access
  - Only **`BCHost`** and local zone renderer have access to *Flash* broker
- How can renderer launch or activate *Flash* broker?

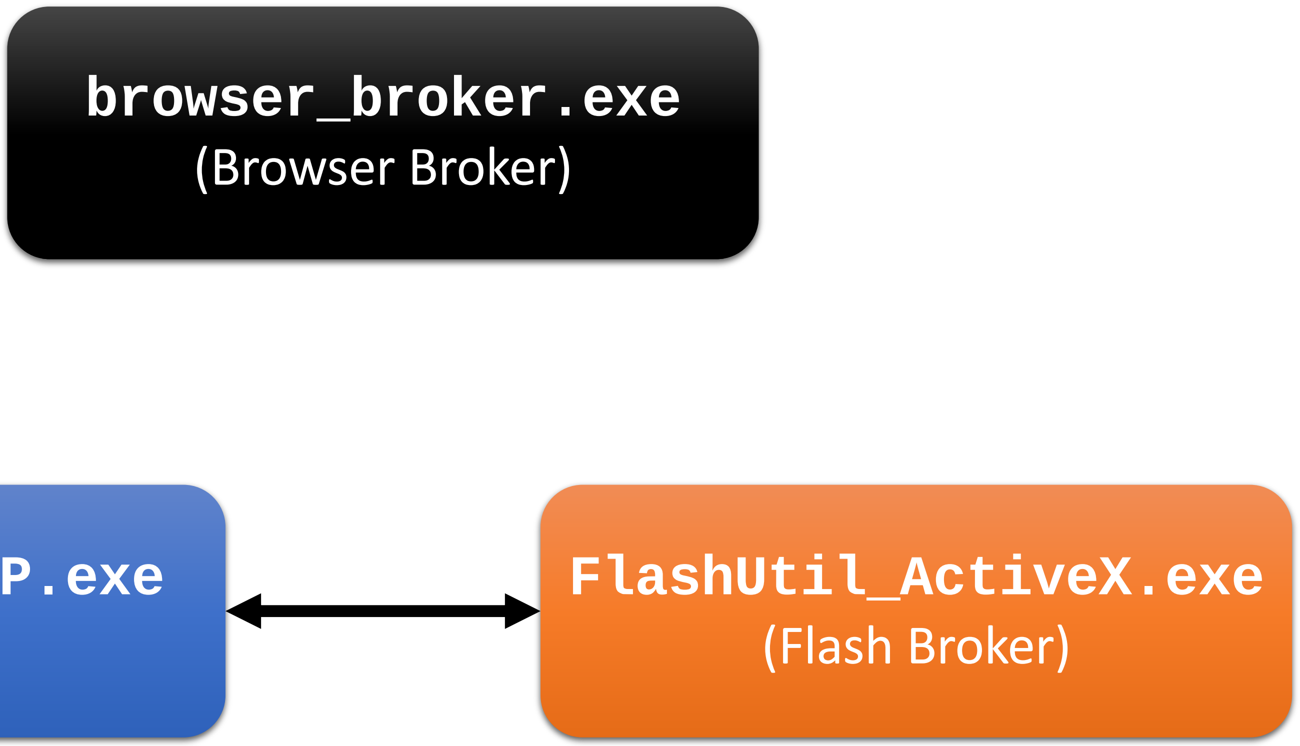
Flash Broker Activation



Flash Broker Activation



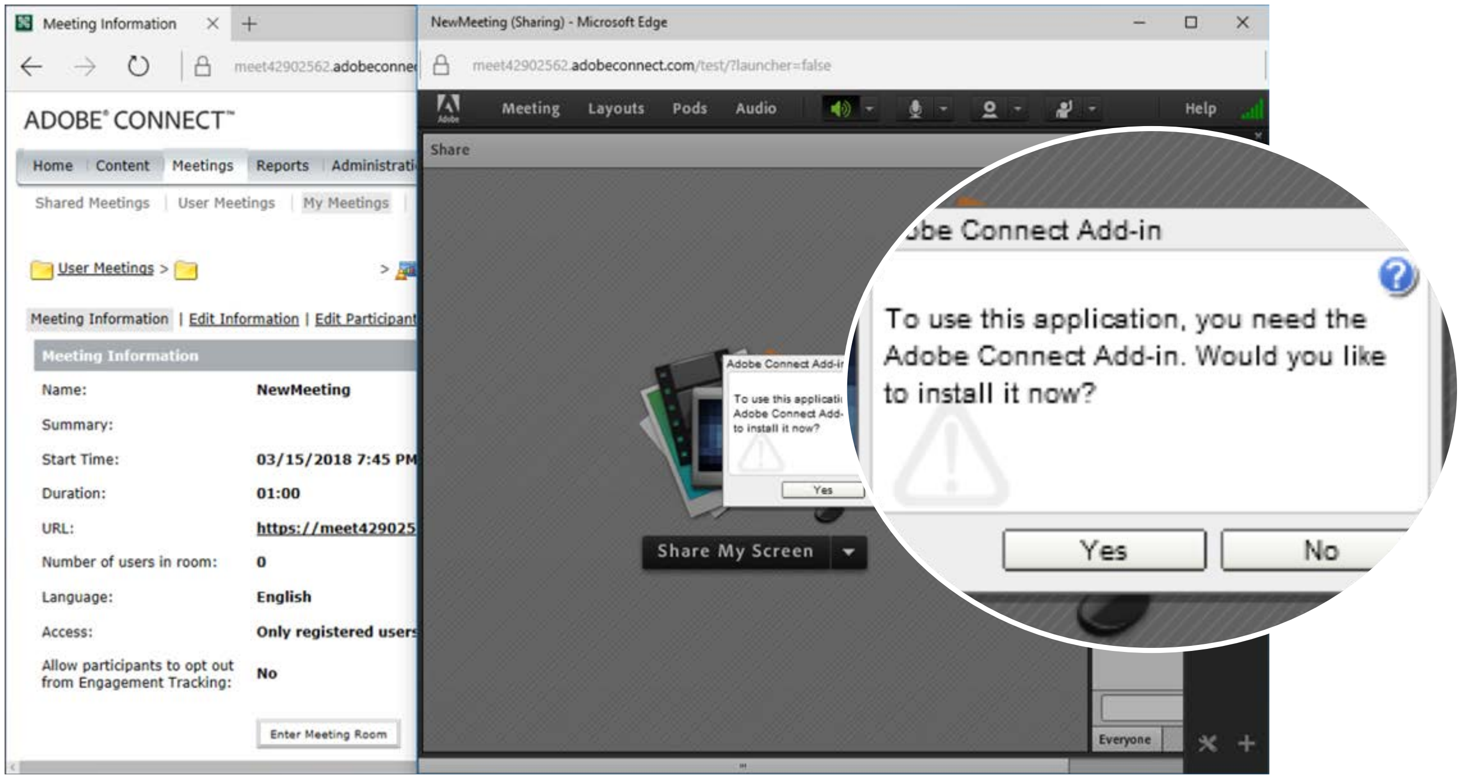
Flash Broker Activation



Flash Broker Features

- *Flash* broker exports 6 interfaces with 124 methods
  - **`IFlashBroker`** : file, LCD accessor, register profile, add-in operations
  - **`IFlashBroker2`**: register profile operations
  - **`IFlashBroker3`**: popup and GDI device operations
  - **`IFlashBroker4`**: utility functionalities
  - **`IFlashBroker5`**: utility functionalities
  - **`IFlashBroker6`**: file operations, add-in operations
- Runs at **Medium Integrity Level**
- Multiple vulnerabilities in last few years
- Is it still insecure?

Adobe Connect Add-in



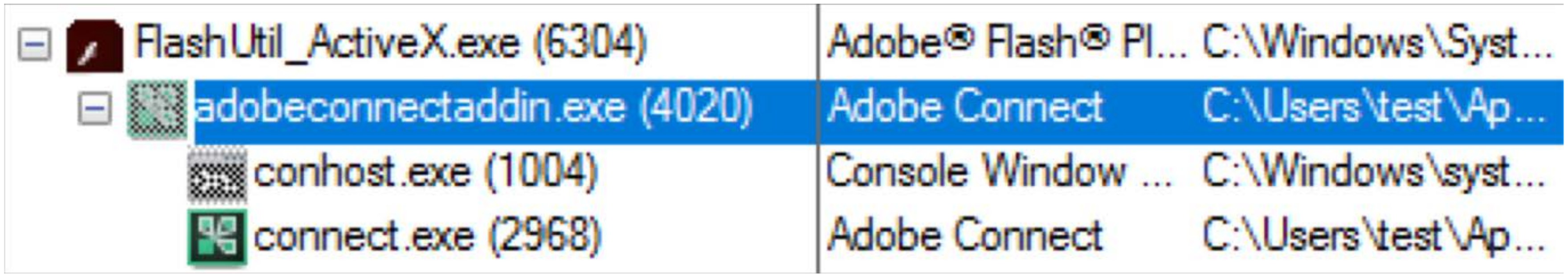
Name:	NewMeeting
Summary:	
Start Time:	03/15/2018 7:45 PM
Duration:	01:00
URL:	https://meet429025
Number of users in room:	0
Language:	English
Access:	Only registered users
Allow participants to opt out from Engagement Tracking:	No

obe Connect Add-in

To use this application, you need the Adobe Connect Add-in. Would you like to install it now?

Yes No

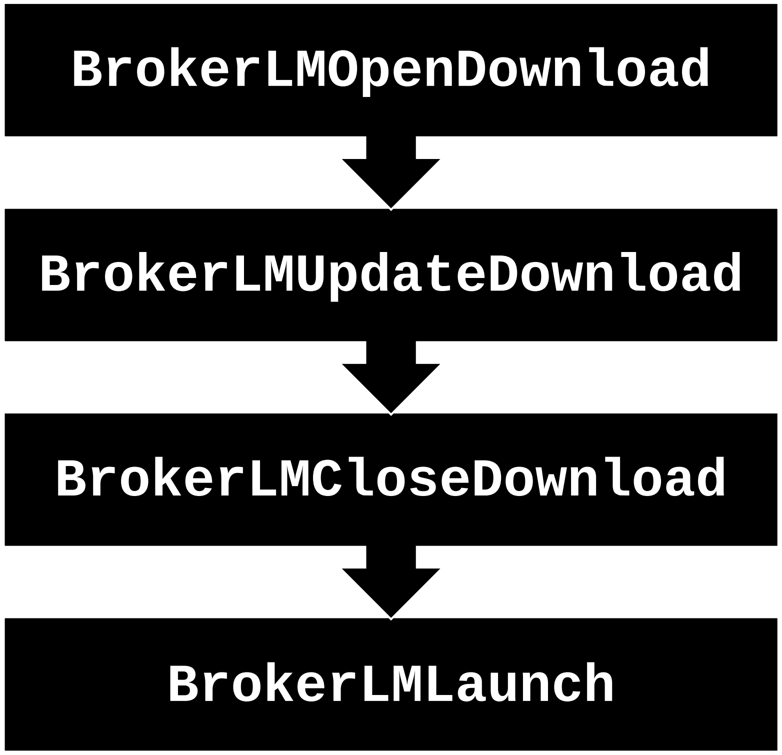
Launch *Macromedia* Add-in



FlashUtil_ActiveX.exe (6304)	Adobe® Flash® Pl...	C:\Windows\Syst...
adobeconnectaddin.exe (4020)	Adobe Connect	C:\Users\test\Ap...
conhost.exe (1004)	Console Window ...	C:\Windows\syst...
connect.exe (2968)	Adobe Connect	C:\Users\test\Ap...

LM Functions in `IFlashBroker6`

- Used for add-in installation
- Check and download files
- Launch the verified add-in
- A pair of files (dot z & dot s file) are downloaded
- The signatures of downloaded files must be valid



Dot Z File

```
30 83 79 D2 AE 06 09 2A 86 48 86 F7 0D 01 07 02
A0 83 79 D2 9E 30 83 79 D2 99 02 01 01 31 0B 30
09 06 05 2B 0E 03 02 1A 05 00 30 83 79 C7 F9 06
09 2A 86 48 86 F7 0D 01 07 01 A0 83 79 C7 E9 04
83 79 C7 E4 54 72 6F 79 D8 B7 F1 00 78 9C EC 7D
73 23 DE 2F 3F 22 18 9C 7A 82 8F 89 51 05 F2 E9
...
```

Adobe Signature

"**Troy**"

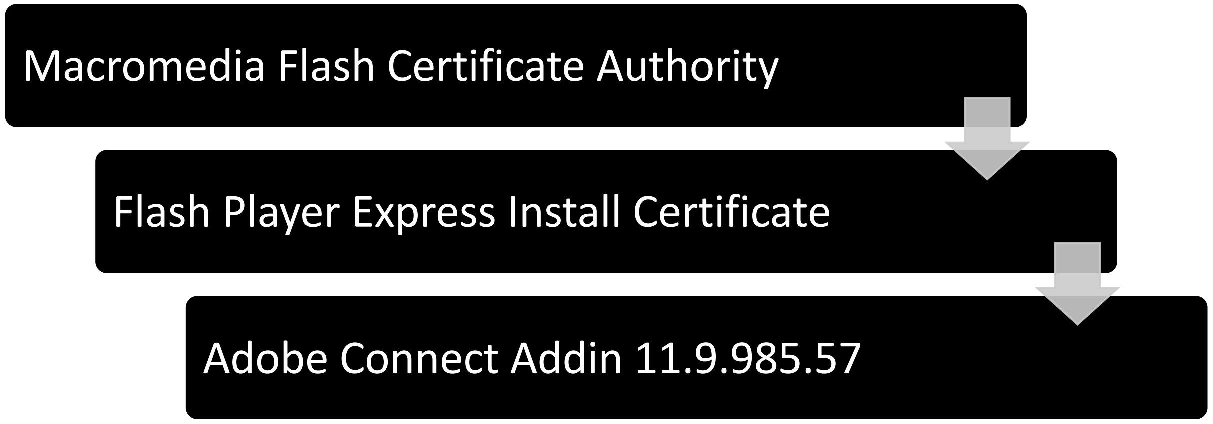
Original File Size

zlib Magic

black hat EUROPE 2018

Dot S File

- Signed by *Adobe*
- Contains a SHA-256 digest used to verify the uncompressed file
- All digital signatures are verified with a built-in certificate
- The certificate chain


Macromedia Flash Certificate Authority
Flash Player Express Install Certificate
Adobe Connect Addin 11.9.985.57

Flash Add-in Download and Launch

Download and verify the dot z file

- URL must be located in “macromedia.com”
- The digital signature of dot z file must be valid

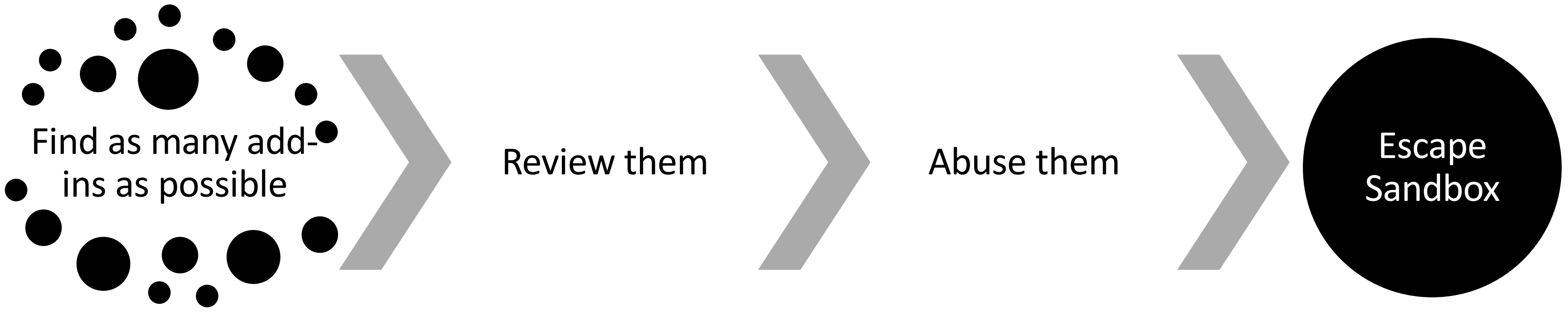
Download the dot s file

- URL must located in “macromedia.com”

Launch add-in with controllable arguments

- The digital signature of dot s file must be valid
- Add-in must match the digest contained in dot s file

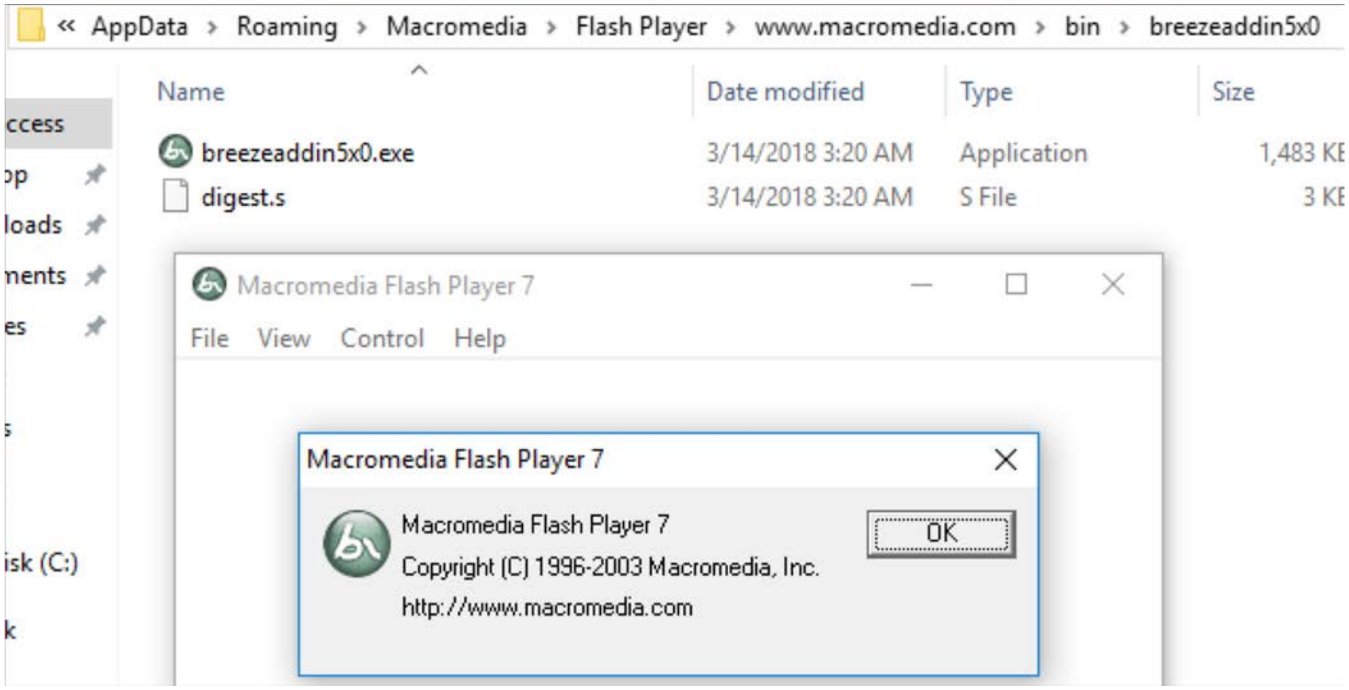
Abusing *Flash* Broker



Vulnerable Add-ins

- Several vulnerable add-ins on the *Macromedia* web server
  - *Macromedia Breeze* 5.0
  - *Cisco Unified MeetingPlace* 6.0
  - *Cisco Unified Presenter* 6.0
  - *Adobe Acrobat Connect* 6.0
  - …
- Add-ins built with an ancient *Adobe Flash Player*
- Add-ins can open a specified SWF file via command line arguments
- We can use known vulnerabilities of *Flash* to escape sandbox

A Bug in *Macromedia Breeze*



« AppData › Roaming › Macromedia › Flash Player › www.macromedia.com › bin › breezeaddin5x0

Name	Date modified	Type	Size
breezeaddin5x0.exe	3/14/2018 3:20 AM	Application	1,483 KE
digest.s	3/14/2018 3:20 AM	S File	3 KE

Macromedia Flash Player 7

Macromedia Flash Player 7
Copyright (C) 1996-2003 Macromedia, Inc.
http://www.macromedia.com

A built-in Flash Player released in the year of 2003

Now What?

How to escape from Internet renderer?

From Attackers' Perspective

- What do we have?
  - Code execution in internet renderer process
  - Sandbox escape in **`BCHost`** or local zone renderer process

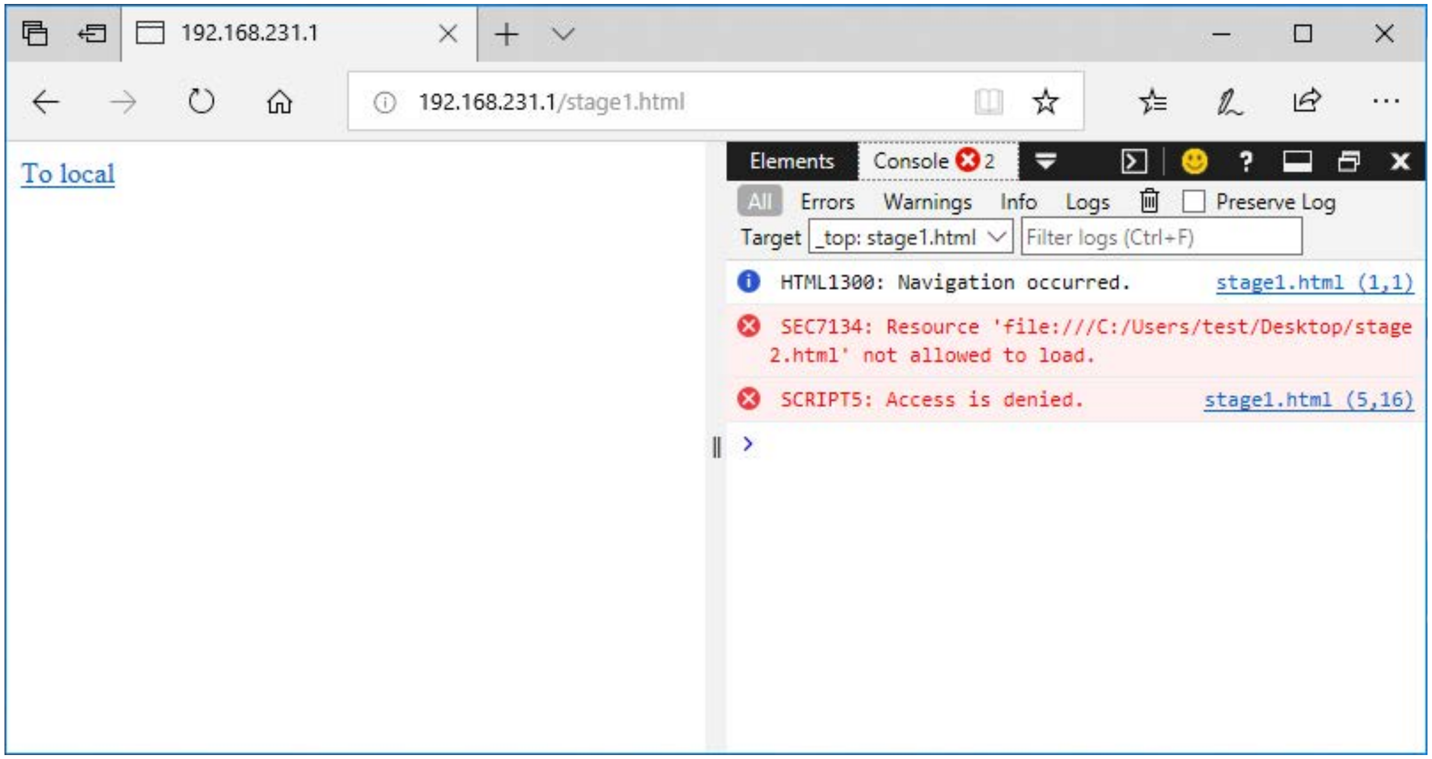
From Attackers’ Perspective

- What do we have?
  - Code execution in internet renderer process
  - Sandbox escape in **`BCHost`** or local zone renderer process
- What do we need?
  - Run JavaScript in **`BCHost`** renderer process
  - Or cross origin from internet to local

From Attackers' Perspective

- What do we have?
  - Code execution in internet renderer process
  - Sandbox escape in **`BCHost`** or local zone renderer process
- What do we need?
  - Run JavaScript in **`BCHost`** renderer process
  - Or cross origin from internet to local
- Running JavaScript in **`BCHost`** renderer needs user confirmation
- UXSS bugs are rare
- What can we do with code execution in renderer?

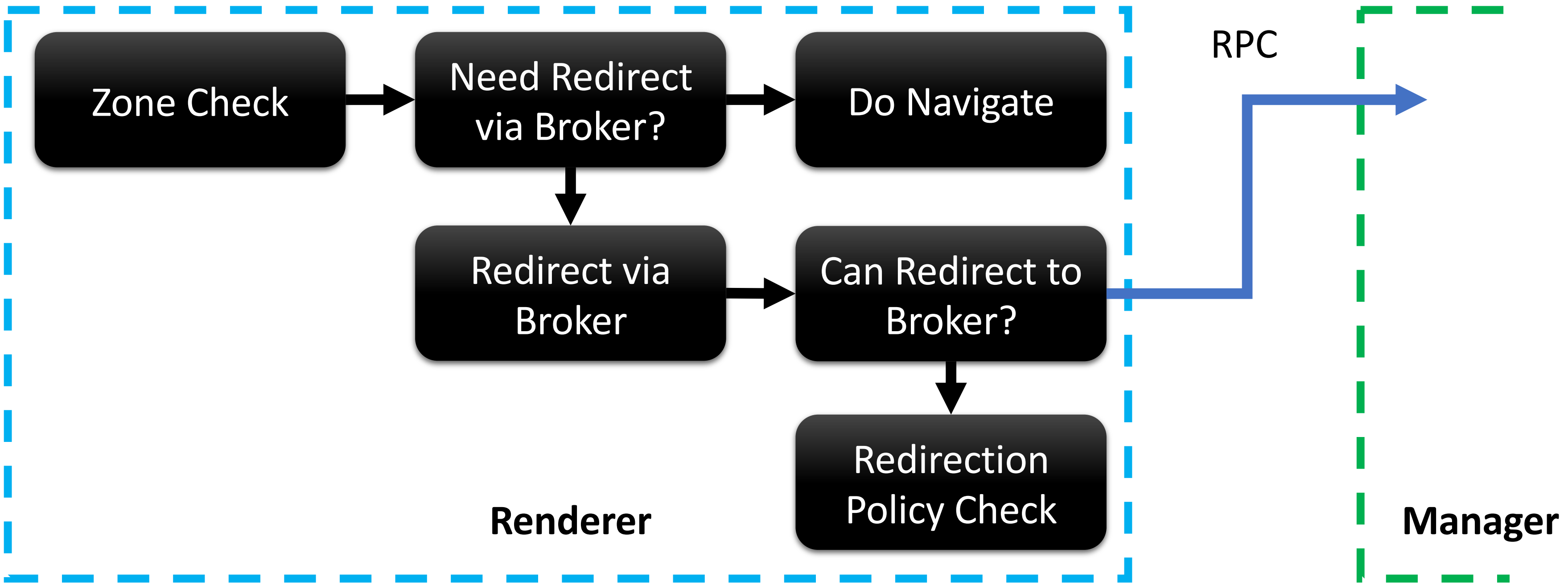
Navigate from Internet Zone to Local Zone Renderer



```
HTML1300: Navigation occurred.                    stage1.html (1,1)
SEC7134: Resource 'file:///C:/Users/test/Desktop/stage
2.html' not allowed to load.
SCRIPT5: Access is denied.                        stage1.html (5,16)
```

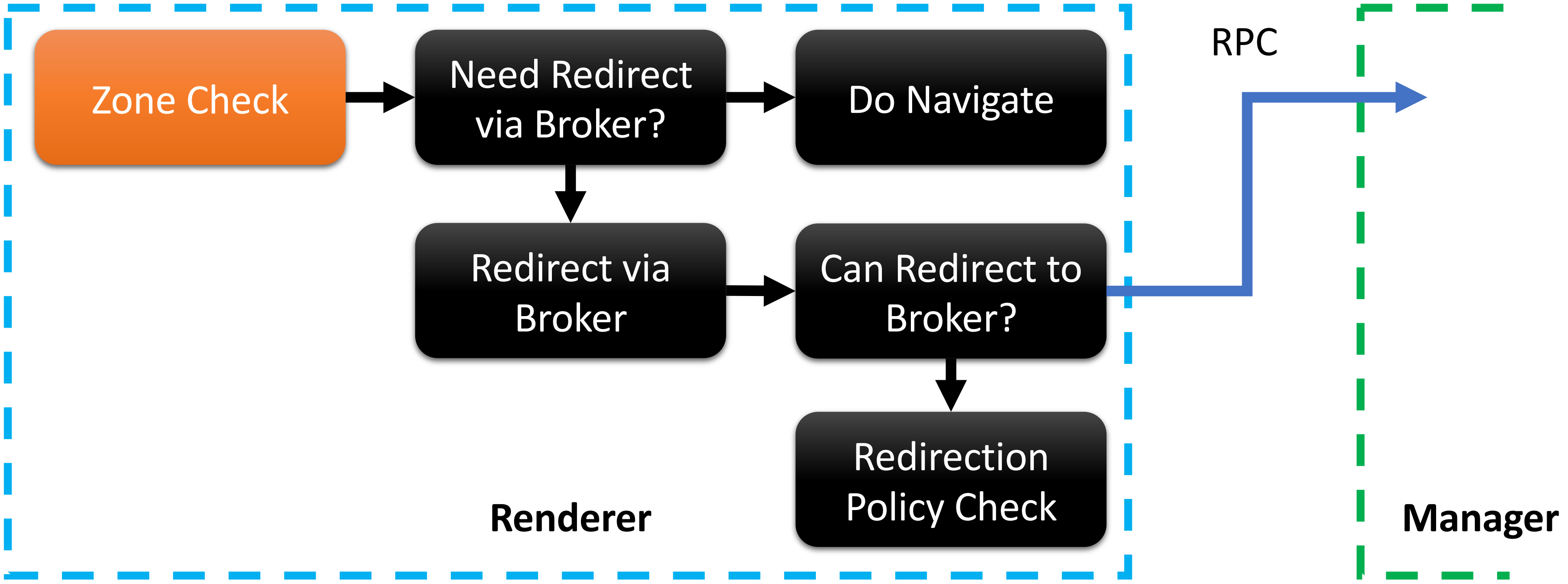
Behind a Navigation

`CDoc::FollowHyperlink2`



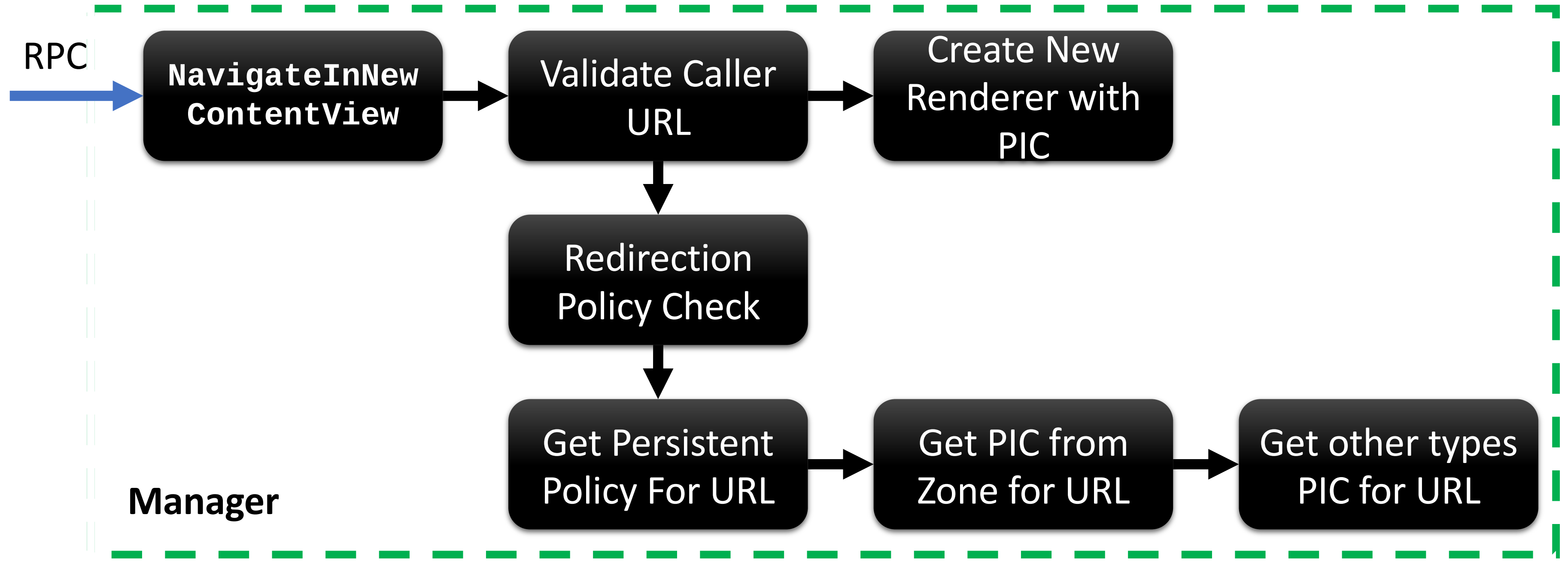
Behind a Navigation

`CDoc::`**`FollowHyperlink2`**



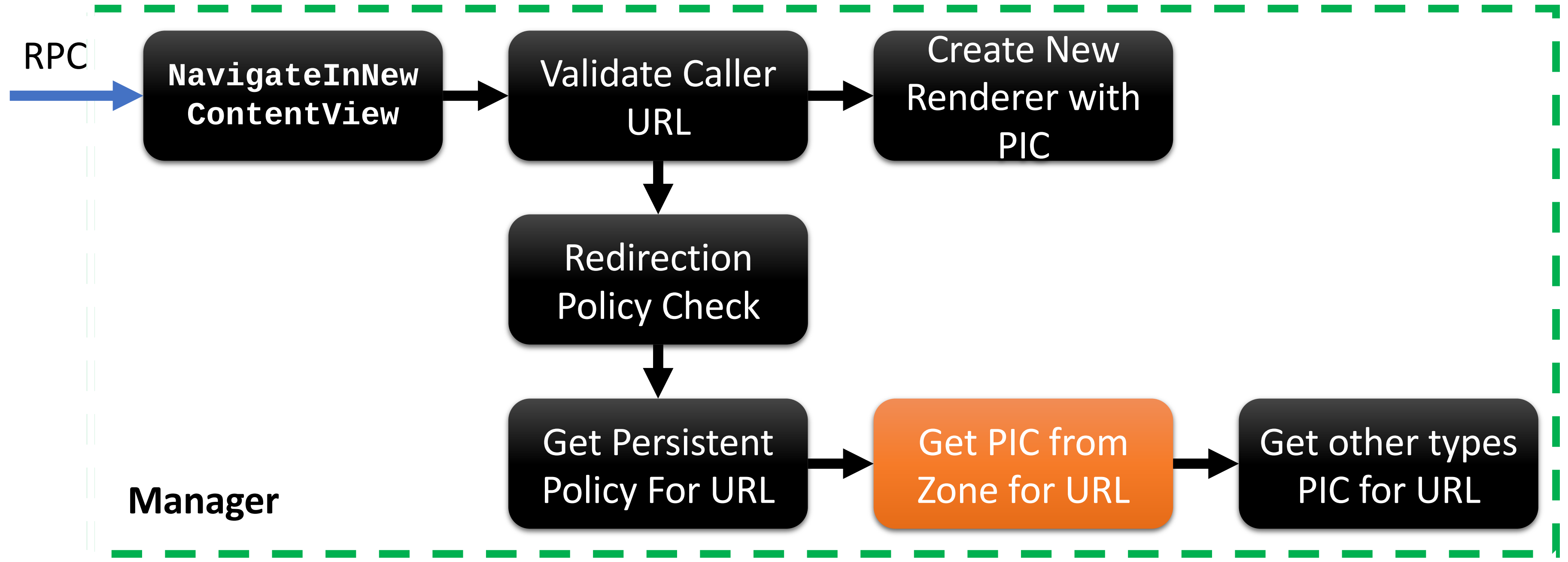
Behind a Navigation

BrowsingContextBroker::**NavigateInNewContentView**


RPC
NavigateInNew ContentView
Validate Caller URL
Create New Renderer with PIC
Redirection Policy Check
Get Persistent Policy For URL
Get PIC from Zone for URL
Get other types PIC for URL
Manager

Behind a Navigation

BrowsingContextBroker::**NavigateInNewContentView**


RPC
NavigateInNewContentView
Validate Caller URL
Create New Renderer with PIC
Redirection Policy Check
Get Persistent Policy For URL
Get PIC from Zone for URL
Get other types PIC for URL
Manager

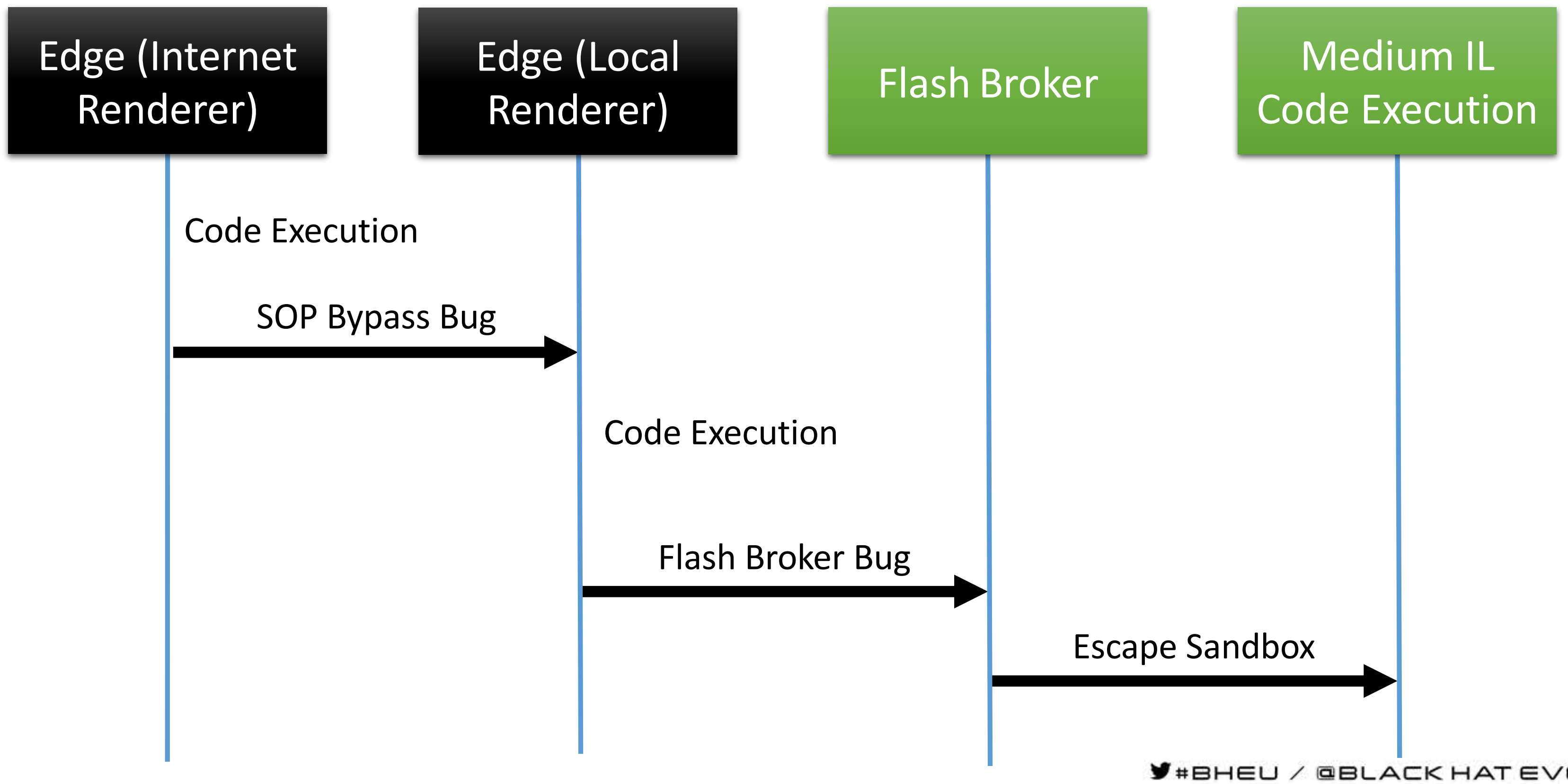
A SOP Bypass

- Zone Check
  - Within renderer
  - Can navigate to a local page when host URL’s protocol is file
  - It can be bypassed with crafted data or request manager directly
- Get PIC from Zone ID for URL
  - Within manager
  - Zone ID is calculated from target URL
  - No additional check for local file URL
- We can render a local HTML file dropped by internet renderer in local zone renderer

Exploit the SOP Bypass

- Write a local HTML file to temporary folder
- Create an **`AnchorElement`** with local HTML file as source
- Locate **`HostUrl`** via the **`AnchorElement`**
- Modify **`HostUrl`** to "**`file:///...`**" to bypass the zone check
- Trigger navigation via **`onclick`** event
- The local HTML file opened in local zone renderer

Put It All Together



Demo

Patches

- For the *Flash* broker bug
  - Removed vulnerable add-ins from macromedia.com
- For the SOP bypass
  - Check file integrity level in `urlmon!`**`IEGetZoneIUri`**
  - Render local HTML files with low integrity level in internet renderer

Recap

- *Microsoft Edge* security architecture Internals
  - How *Microsoft* mitigated a class of bugs by reducing attack surface
- *Microsoft Edge* Inter-process communication mechanisms
- 3 sandbox escape chains used in *Pwn2Own*
  - Browser Broker bug
  - Flash Broker bug
  - SOP bypass

Black Hat Sound Bytes

Logical bugs comes from bad design decisions

Finding logical bugs requires deep knowledge of internals, even deeper than developers

Logical bugs are beautiful, useful and fun

Special Thanks

- Alex Ionescu (@aionescu)
- James Forshaw (@tiraniddo)
- Yang Yu (@tombkeeper)

Thanks.

Tencent Security Xuanwu Lab

@XuanwuLab

xlab.tencent.com

Credits and References

- Wikimedia Commons
  - *Microsoft Edge* icon
  - *Adobe Flash Player* icon
  - Trojan horse
- Diving into IE10's Enhanced Protected Mode Sandbox
  Mark Vincent Yason